7ª Edición

Comunicaciones y Redes de Computadores

PEARSON
Prentice Hall

William Stallings

COMUNICACIONES Y REDES DE COMPUTADORES

Séptima edición

COMUNICACIONES Y REDES DE COMPUTADORES

Séptima edición

William Stallings

Traducción:

Jesús Esteban Díaz Verdejo
Juan Manuel Estévez Tapiador
Pedro García Teodoro
Juan Manuel López Soler
Juan José Ramos Muñoz
Área de Ingeniería Telemática
Universidad de Granada

Revisión Técnica:

Raúl V. Ramírez Velarde
Profesor asociado
Departamento de Ciencias Computacionales
Instituto Tecnológico y de Estudios Superiores de Monterrey
Campos Monterrey - México

M. en C. Jaquelina López Barrientos
Profesora de Tiempo Completo
Departamento de Ingeniería en Computación
Facultad de Ingeniería
Universidad Nacional Autónoma de México

Madrid • México • Santafé de Bogotá • Buenos Aires • Caracas • Lima • Montevideo
San Juan • San José • Santiago • São Paulo • White Plains

Datos de catalogaci n bibliogr fica

STALLINGS, WILLIAM
COMUNICACIONES Y REDES DE COMPUTADORES
Séptima edición

PEARSON EDUCACIÓN, S.A., Madrid, 2004

ISBN: 978-84-205-4110-5
Materia: Informática 681.3

Formato 195 × 250 Páginas: 896

STALLINGS, WILLIAM
***COMUNICACIONES Y REDES DE COMPUTADORES*. Séptima edición**

Todos los derechos reservados.
Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (*arts*. 270 *y sgts*. *Código Penal*).

DERECHOS RESERVADOS
© 2004 por PEARSON EDUCACIÓN, S.A.
Ribera del Loira, 28
28042 MADRID (España)

PEARSON PRENTICE HALL es un sello editorial autorizado de PEARSON EDUCACIÓN, S.A.

Authorized translation from the English language edition, entitled DATA AND COMPUTER COMMUNICATIONS, 7th Edition by STALLINGS, WILLIAM.
Published by Pearson Education, Inc, publishing as Prentice Hall
© 2004. All rights reserved.
No part of this book may be reproduced or transmitted in any form or by any means, electronic of mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

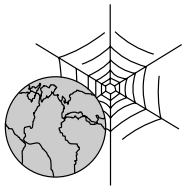
ISBN: 978-84-205-4110-5
Depósito legal: M. 14.542-2008

Última reimpresión, 2008

Equipo editorial:
Editor: David Fayerman Aragón
Técnico editorial: Ana Isabel García Borro
Equipo de producción:
Director: José Antonio Clares
Técnico: José Antonio Hernán
Diseño de cubierta: Equipo de diseño de PEARSON EDUCACIÓN, S.A.
Composición: COPIBOOK, S.L.

IMPRESO EN MÉXICO - PRINTED IN MEXICO

A mi brillante esposa ATS



SERVIDOR WEB PARA EL LIBRO «COMUNICACIONES Y REDES DE COMPUTADORES» *Séptima edición.*

En la dirección web **http://www.williamstallings.com/DCC/DCC7e.html** se encuentra diverso material de ayuda para los profesores y estudiantes que utilicen este libro. Incluye los siguientes elementos [1].

Materiales de ayuda para impartir cursos

Los elementos de ayuda para impartir cursos son:

- Copia de las figuras del libro en formato PDF.
- Conjunto detallado de notas en formato PDF adecuado como apuntes de los alumnos o para usar como esquemas.
- Conjunto de transparencias/diapositivas en PowerPoint como ayuda para impartir las clases.
- Páginas de ayuda a los estudiantes de computación: contienen gran cantidad de enlaces y documentos que los estudiantes pueden encontrar útiles para su actualización de conocimientos en computación. Se incluye una revisión de los conceptos básicos relevantes de matemáticas, consejos sobre la realización de los problemas, enlaces a recursos de investigación como depósito de informes y referencias bibliográficas y otros enlaces útiles.
- Una fe de erratas del libro, actualizada al menos mensualmente.

Cursos sobre comunicaciones y redes de computadores

El servidor web DCC7e incluye enlaces a páginas web que tratan sobre cursos relacionados con el libro. Estos sitios suministran ideas muy útiles sobre la planificación y ordenación de los temas, así como diversos apuntes y otros materiales.

[1] *N. del T.:* estas páginas web, que son regularmente actualizadas, se encuentran en el idioma original del libro (inglés).

Páginas web útiles

El servidor DCC7e incluye enlaces a sitios web relevantes, organizados por capítulos. Los enlaces abarcan un amplio espectro de tópicos y posibilitan la exploración puntual de temas en gran profundidad por parte del alumno.

Documentos suplementarios

El servidor DCC7e incluye varios documentos que amplían lo tratado en el libro. Entre los temas ampliados se encuentran las organizaciones de estandarización, los *sockets*, la suma de comprobación de TCP/IP, ASCII y el teorema de muestreo.

Lista de correo internet

Se mantiene una lista de direcciones de correo electrónico para que los profesores que utilizan el libro puedan intercambiar información, sugerencias y dudas entre ellos y con el autor. La información necesaria para ser incluido en esta lista se encuentra en la página web.

Herramientas de modelado y simulación

La página web incluye enlaces a los servidores web de *cnet* y *modeling tools*. Estos paquetes pueden utilizarse para analizar y experimentar con problemas de protocolos y diseño de redes. Cada servidor incluye software transferible al equipo del usuario e información básica. El manual del profesor contiene mayor información sobre cómo copiar y usar el software y propuestas de proyectos a realizar por los estudiantes. *Véase* el Apéndice D para más información.

Contenido

Prólogo XXIII

Capítulo 0. Guía del lector 1

0.1. Resumen del texto 2

0.2. Internet y recursos web 2
Sitios web relacionados con el texto 2
Otros sitios web 3
Grupos de noticias de USENET 4

0.3. Estándares 4

PARTE I
Descripción general

Capítulo 1. Introducción a las comunicaciones de datos y redes 9

1.1. Un modelo para las comunicaciones 10

1.2. Comunicaciones de datos 13

1.3. Redes de transmisión de datos 14
Redes de área amplia 15
Redes de área local 17
Redes inalámbricas 17
Redes de área metropolitana 17

1.4. Un ejemplo de configuración 18

Capítulo 2. Arquitectura de protocolos 21

2.1. ¿Por qué es necesaria una arquitectura de protocolos? 22

2.2. Una arquitectura de protocolos simple 23
Un modelo de tres capas 25
Arquitecturas de protocolos normalizadas 28

2.3. OSI 29
El modelo 29
Normalización dentro del modelo de referencia OSI 32
Parámetros y primitivas de servicio 35
Las capas de OSI 36
2.4. La arquitectura de protocolos TCP/IP 40
Las capas de TCP/IP 40
TCP y UDP 41
Funcionamiento de TCP e IP 42
Aplicaciones TCP/IP 44
Interfaces de protocolo 45
2.5. Lecturas recomendadas y sitios web 45
Sitios web recomendados 46
2.6. Términos clave, cuestiones de repaso y ejercicios 47
Términos clave 47
Cuestiones de repaso 47
Ejercicios 47
Apéndice 2A. El protocolo TFTP (*Trivial File Transfer Protocol*) 49
Introducción a TFTP 49
Paquetes TFTP 49
Ejemplo de transferencia 51
Errores y retardos 51
Sintaxis, semántica y temporización 52

PARTE II
Comunicaciones de datos

Capítulo 3. Transmisión de datos 57
3.1. Conceptos y terminología 59
Terminología utilizada en transmisión de datos 59
Frecuencia, espectro y ancho de banda 59
3.2. Transmisión de datos analógicos y digitales 69
Datos analógicos y digitales 69
Señales analógicas y digitales 72
Transmisión analógica y digital 76
3.3. Dificultades en la transmisión 78
Atenuación 78
Distorsión de retardo 80
Ruido 80
3.4. Capacidad del canal 83
Ancho de banda de Nyquist 84
Fórmula para la capacidad de Shannon 84
El cociente E_b/N_0 86
3.5. Lecturas recomendadas 88
3.6. Términos clave, cuestiones de repaso y ejercicios 88
Términos clave 88
Cuestiones de repaso 88
Ejercicios 89
Apéndice 3A. Decibelios y energía de la señal 91

Capítulo 4. Medios de transmisión 95

4.1. Medios de transmisión guiados 97
Par trenzado 99
Cable coaxial 104
Fibra óptica 105

4.2. Transmisión inalámbrica 109
Antenas 110
Microondas terrestres 112
Microondas por satélite 113
Ondas de radio 116
Infrarrojos 117

4.3. Propagación inalámbrica 117
Propagación superficial de ondas 119
Propagación aérea de ondas 120
Propagación en la trayectoria visual 120

4.4. Transmisión en la trayectoria visual 122
Pérdida en el espacio libre 122
Absorción atmosférica 124
Multitrayectorias 125
Refracción 126

4.5. Lecturas recomendadas y sitios web 126

4.6. Términos clave, cuestiones de repaso y ejercicios 127
Términos clave 127
Cuestiones de repaso 127
Ejercicios 128

Capítulo 5. Técnicas para la codificación de señales 133

5.1. Datos digitales, señales digitales 135
No retorno a cero 139
Binario multinivel 140
Bifase 141
Velocidad de modulación 143
Técnicas de aleatorización 144

5.2. Datos digitales, señales analógicas 146
Modulación por desplazamiento de amplitud 146
Modulación por desplazamiento de frecuencia 147
Modulación por desplazamiento de fase 149
Prestaciones 153
Modulación de amplitud en cuadratura 156

5.3. Datos analógicos, señales digitales 157
Modulación por impulsos codificados 157
Modulación delta 160
Prestaciones 162

5.4. Datos analógicos, señales analógicas 163
Modulación de amplitud 164
Modulación angular 166

5.5. Lecturas recomendadas 169

5.6. Términos clave, cuestiones de repaso y ejercicios 170
Términos clave 170
Cuestiones de repaso 171
Ejercicios 171

Capítulo 6. Técnicas de comunicación de datos digitales 177

6.1. Transmisión asíncrona y síncrona 179
Transmisión asíncrona 179
Transmisión síncrona 181

6.2. Tipos de errores 182

6.3. Detección de errores 183
Comprobación de paridad 184
Comprobación de redundancia cíclica (CRC) 185

6.4. Corrección de errores 191
Principios generales de los códigos de bloque 193

6.5. Configuraciones de línea 197
Topología 197
Full-duplex y *Half-duplex* 197

6.6. Interfaces 198
V.24/EIA-232-F 200
La interfaz física de RDSI 206

6.7. Lecturas recomendadas 209

6.8. Términos clave, cuestiones de repaso y ejercicios 210
Cuestiones de repaso 210
Ejercicios 210

Capítulo 7. Protocolos de control del enlace de datos 215

7.1. Control de flujo 217
Control de flujo mediante parada y espera 218
Control de flujo mediante ventana deslizante 220

7.2. Control de errores 223
ARQ con parada y espera 224
ARQ con vuelta atrás N 226
ARQ con rechazo selectivo 228

7.3. Control del enlace de datos de alto nivel (HDLC) 229
Características básicas 229
Estructura de trama 230
Funcionamiento 233

7.4. Lecturas recomendadas 237

7.5. Términos clave, cuestiones de repaso y ejercicios 237
Términos clave 237
Cuestiones de repaso 238
Ejercicios 238

Apéndice 7A. Análisis de prestaciones 241
Control del flujo mediante parada y espera 241
Control del flujo sin errores mediante ventana deslizante 243
ARQ 245

Capítulo 8. Multiplexación 249

8.1. Multiplexación por división en frecuencias 251
Características 251
Sistemas de portadora analógica 256
Multiplexación por división en la longitud de onda 257

8.2. Multiplexación por división en el tiempo síncrona 258
Características 258
Control del enlace en TDM 260
Sistemas de portadora digital 263
SONET/SDH 265

8.3. Multiplexación por división en el tiempo estadística 268
Características 268
Prestaciones 270
Cable-módem 274

8.4. Línea de abonado digital asimétrica 275
Diseño ADSL 275
Multitono discreto 277

8.5. xDSL 278
Línea de abonado digital de alta velocidad (HDSL) 278
Línea de abonado digital de una sola línea (SDSL) 279
Línea de abonado digital de muy alta velocidad (VDSL) 279

8.6. Lecturas y sitios web recomendados 280

8.7. Términos clave, cuestiones de repaso y ejercicios 280
Términos clave 280
Cuestiones de repaso 281
Ejercicios 281

Capítulo 9. Espectro expandido 285

9.1. El concepto de espectro expandido 286

9.2. Espectro expandido por salto de frecuencias 287
Esquema básico 288
FHSS usando MFSK 290
Análisis de prestaciones de FHSS 292

9.3. Espectro expandido de secuencia directa 292
DSSS usando BPSK 293
Análisis de prestaciones de DSSS 294

9.4. Acceso múltiple por división de código 297
Principios básicos 297
CDMA para espectro expandido de secuencia directa 299

9.5. Lecturas recomendadas 300

9.6. Términos clave, cuestiones de repaso y ejercicios 301
Términos clave 301
Cuestiones de repaso 301
Ejercicios 301

PARTE III
Redes de área amplia

Capítulo 10. Conmutación de circuitos y de paquetes 309

10.1. Redes conmutadas 311

10.2. Redes de conmutación de circuitos 312

10.3. Conceptos de conmutación de circuitos 315
Conmutación por división en el espacio 317
Conmutación por división en el tiempo 319

10.4. Señalización de control 319
Funciones de señalización 320
Localización de la señalización 322
Señalización por canal común 322
Sistema de señalización número 7 326

10.5. Arquitectura de conmutación lógica 329

10.6. Principios de conmutación de paquetes 330
Técnica de conmutación 331
Tamaño de paquete 334
Comparación de las técnicas de conmutación de circuitos y de paquetes 336

10.7. X.25 339

10.8. Retransmisión de tramas 341
Fundamentos 341
Arquitectura de protocolos en retransmisión de tramas 342
Transferencia de datos de usuario 343

10.9. Lecturas y sitios web recomendados 345

10.10. Términos clave, cuestiones de repaso y ejercicios 346
Términos clave 346
Cuestiones de repaso 346
Ejercicios 347

Capítulo 11. Modo de transferencia asíncrono 349

11.1. Arquitectura de protocolos 350

11.2. Conexiones lógicas ATM 351
Uso de conexiones de canal virtual 353
Características camino virtual/canal virtual 354
Señalización de control 355

11.3. Celdas ATM 356
Formato de cabecera 356
Control de flujo genérico 358
Control de errores de cabecera 360

11.4. Transmisión de celdas ATM 362
Capa física basada en celdas 362
Capa física basada en SDH 364

11.5. Clases de servicios ATM 365
Servicios en tiempo real 365
Servicios en no tiempo real 366

11.6. Capa de adaptación ATM 368
Servicios AAL 368
Protocolos AAL 370

11.7. Lecturas y sitios web recomendados 375

11.8. Términos clave, cuestiones de repaso y ejercicios 376
Términos clave 376
Cuestiones de repaso 376
Ejercicios 376

Capítulo 12. Encaminamiento en redes conmutadas 379

12.1. Encaminamiento en redes de conmutación de circuitos 380

12.2. Encaminamiento en redes de conmutación de paquetes 382
Características 382
Estrategias de encaminamiento 386
Ejemplos 391

12.3. Algoritmos de mínimo coste 397
Algoritmo de Dijkstra 397
Algoritmo de Bellman-Ford 398
Comparación 401

12.4. Lecturas recomendadas 401

12.5. Términos clave, cuestiones de repaso y ejercicios 401
Términos clave 401
Cuestiones de repaso 402
Ejercicios 402

Capítulo 13. Congestión en redes de datos 407

13.1. Efectos de la congestión 409
Funcionamiento ideal 410
Funcionamiento real 412

13.2. Control de congestión 413
Contrapresión 414
Paquetes de obstrucción 414
Señalización implícita de congestión 415
Señalización explícita de congestión 415

13.3. Gestión de tráfico 416
Imparcialidad 417
Calidad de servicio 417
Reservas 417

13.4. Control de congestión en redes de conmutación de paquetes 418

13.5. Control de congestión en retransmisión de tramas 418
Gestión de la tasa de tráfico 420
Prevención de congestión mediante señalización explícita 423

13.6. Gestión de tráfico en ATM 424
Requisitos para el control de tráfico y de congestión en ATM 424
Efectos de latencia/velocidad 425
Variación del retardo de celdas 426

Control de tráfico y de congestión 429
Técnicas de gestión de tráfico y de control de congestión 430

13.7. Gestión de tráfico GFR en ATM 436
Mecanismos de soporte de tasas garantizadas 437
Definición de adecuación GFR 438
Mecanismo para la comprobación de elegibilidad de QoS 439

13.8. Lecturas recomendadas 439

13.9. Términos clave, cuestiones de repaso y ejercicios 441
Términos clave 441
Cuestiones de repaso 441
Ejercicios 441

Capítulo 14. Redes celulares inalámbricas 445

14.1. Principios de redes celulares 446
Organización de una red celular 446
Funcionamiento de sistemas celulares 451
Efectos de propagación en radio móvil 454
Desvanecimiento en entornos móviles 456

14.2. Primera generación analógica 460
Asignación espectral 460
Funcionamiento 461
Canales de control en AMPS 461

14.3. CDMA de segunda generación 461
Sistemas celulares de primera y segunda generación 462
Acceso múltiple por división de código 462
Consideraciones de diseño de CDMA móvil inalámbrico 463
IS-95 464
Enlace de ida en IS-95 464
Enlace de retorno en IS-95 467

14.4. Sistemas de tercera generación 470
Interfaces alternativas 471
Consideraciones de diseño de CDMA 472

14.5. Lecturas y sitios web recomendados 473

14.6. Términos clave, cuestiones de repaso y ejercicios 474
Términos clave 474
Cuestiones de repaso 475
Ejercicios 475

PARTE IV
Redes de área local

Capítulo 15. Visión general de las redes de área local 479

15.1. Aplicaciones de las redes LAN 480
Redes LAN de computadores personales 480
Redes de respaldo y almacenamiento 481
Redes ofimáticas de alta velocidad 483
Redes LAN troncales 483

15.2. Topologías y medios de transmisión 484
Topologías 484
Elección de la topología 488
Elección del medio de transmisión 489

15.3. Arquitectura de protocolos de redes LAN 489
Modelo de referencia IEEE 802 490
Control del enlace lógico 492
Control de acceso al medio 495

15.4. Puentes 497
Funciones de los puentes 498
Arquitectura de protocolos de los puentes 499
Encaminamiento estático 500
Técnica del árbol de expansión 502

15.5. Conmutadores de la capa 2 y la capa 3 504
Concentradores 504
Conmutadores de la capa 2 505
Conmutadores de la capa 3 508

15.6. Lecturas y sitios web recomendados 510

15.7. Términos clave, cuestiones de repaso y ejercicios 510
Términos clave 510
Cuestiones de repaso 510
Ejercicios 511

Capítulo 16. Redes LAN de alta velocidad 513

16.1. Surgimiento de las redes LAN de alta velocidad 515

16.2. Ethernet 516
Control de acceso al medio en IEEE 802.3 516
Especificaciones IEEE 802.3 10 Mbps (Ethernet) 522
Especificaciones IEEE 802.3 100 Mbps (Fast Ethernet) 513
Gigabit Ethernet 526
Ethernet de 10 Gpbs 519

16.3. Anillo con paso de testigo 530
Funcionamiento del anillo 530
Control de acceso al medio 532
Opciones de medios de transmisión en IEEE 802.5 534

16.4. Canal de fibra 535
Elementos del canal de fibra 536
Arquitectura de protocolos del canal de fibra 537
Medios físicos y topologías del canal de fibra 537
Perspectivas del canal de fibra 539

16.5. Lecturas y sitios web recomendados 539

16.6. Términos clave, cuestiones de repaso y ejercicios 540
Términos clave 540
Cuestiones de repaso 541
Ejercicios 541

Apéndice 16A. Codificación de señales digitales para redes LAN 543
4B/5B-NRZI 543
MLT-3 545
8B6T 546
8B/10B 548

Apéndice 16B. Análisis de prestaciones 548
Efecto del retardo de propagación y la velocidad de transmisión 549
Modelos sencillos de eficiencia para las técnicas de paso de testigo y CSMA/CD 552

Capítulo 17. Redes LAN inalámbricas 557

17.1. Visión general 558
Aplicaciones de las redes LAN inalámbricas 558
Requisitos de las redes LAN inalámbricas 561

17.2. Tecnología LAN inalámbrica 563
Redes LAN de infrarrojos 563
Redes LAN de espectro expandido 565
Redes LAN de microondas de banda estrecha 566

17.3. Arquitectura y servicios de IEEE 802.11 567
Arquitectura de IEEE 802.11 567
Servicios de IEEE 802.11 569

17.4. Control de acceso al medio en IEEE 802.11 572
Entrega fiable de datos 572
Control de acceso 573
Trama MAC 577

17.5. Capa física de IEEE 802.11 579
Capa física original de IEEE 802.11 580
IEEE 802.11a 581
IEEE 802.11b 581
IEEE 802.11g 581

17.6. Lecturas y sitios web recomendados 582

17.7. Términos clave y cuestiones de repaso 583
Términos clave 583
Cuestiones de repaso 583

PARTE V
Protocolos de interconexión

Capítulo 18. Protocolos de interconexión de redes 587

18.1. Funciones básicas de los protocolos 588
Encapsulamiento 589
Fragmentación y reensamblado 589
Control de conexión 590
Entrega ordenada 592
Control de flujo 592
Control de errores 592
Direccionamiento 593
Multiplexación 595
Servicios de transmisión 596

18.2. Principios de la interconexión entre redes 597
Requisitos 598
Enfoques sobre la arquitectura 599

18.3. Interconexión entre redes sin conexión 600
Funcionamiento de un esquema de interconexión no orientado a conexión 601
Cuestiones de diseño 603

18.4. El protocolo Internet 608
Servicios IP 608
Protocolo IP 609
Direcciones IP 611
Protocolo de mensajes de control de internet (ICMP) 614

18.5. IPv6 617
IP de nueva generación 617
Estructura IPv6 619
Cabecera IPv6 620
Direcciones IPv6 623
Cabecera de opciones salto a salto 624
Cabecera de fragmentación 626
Cabecera de encaminamiento 626
Cabecera de opciones para el destino 627

18.6. Lecturas y sitios web recomendados 627

18.7. Términos clave, cuestiones de repaso y ejercicios 628
Términos clave 628
Cuestiones de repaso 628
Ejercicios 628

Capítulo 19. Funcionamiento de la interconexión de redes 631

19.1. Multidifusión 633
Requisitos para la multidifusión 635
Protocolo de gestión de grupos de Internet 638

19.2. Protocolos de encaminamiento 642
Sistemas autónomos 642
Estrategias de encaminamiento 644
Protocolo de pasarela frontera 645
Protocolo del primer camino más corto disponible 651

19.3. Arquitectura de servicios integrados 654
Tráfico en Internet 654
Enfoque ISA 657
Componentes ISA 658
Servicios ISA 659
Disciplinas de atención de cola 662
Protocolo de reserva de recursos 663

19.4. Servicios diferenciados 665
Servicios 666
Octeto DS 668
Configuración y funcionamiento de los DS 670
Comportamiento por salto 672

19.5. Lecturas y sitios web recomendados 674

19.6. Términos clave, cuestiones de repaso y ejercicios 676
Términos clave 676
Cuestiones de repaso 677
Ejercicios 677

Capítulo 20. Protocolos de transporte 679

20.1. Mecanismos de los protocolos de transporte orientados a conexión 680
Servicio de red de entrega ordenada fiable 681
Servicio de red no fiable 689

20.2. TCP 699
Servicios TCP 699
Formato de la cabecera TCP 699
Mecanismos TCP 703
Opciones en los criterios de implementación de TCP 705

20.3. Control de congestión de TCP 707
Gestión de temporizadores de retransmisión 707
Gestión de ventana 714

20.4. UDP 716

20.5. Lecturas recomendadas 718

20.6. Términos clave, cuestiones de repaso y ejercicios 718
Términos clave 718
Cuestiones de repaso 718
Ejercicios 719

Capítulo 21. Seguridad en redes 723

21.1. Requisitos de seguridad y ataques 725
Ataques pasivos 725
Ataques activos 726

21.2. Privacidad con cifrado simétrico 726
Cifrado simétrico 727
Algoritmos de cifrado 728
Localización de los dispositivos de cifrado 732
Distribución de claves 733
Relleno de tráfico 735

21.3. Autenticación de mensajes y funciones de dispersión («hash») 735
Alternativas para la autenticación de mensajes 735
Funciones de dispersión seguras 739
La función de dispersión segura SHA-1 740

21.4. Cifrado de clave pública y firmas digitales 742
Cifrado de clave pública 742
Firma digital 744
El algoritmo de cifrado de clave pública RSA 745
Gestión de claves 748

21.5. Capa de sockets segura (SSL) y capa de transporte segura (TLS) 749
Arquitectura SSL 749
Protocolo de registro de SSL 750

Protocolo de cambio de especificación de cifrado 751
Protocolo de alerta 752
Protocolo de negociación bilateral 752

21.6. Seguridad en IPv4 e IPv6 754
Aplicaciones de IPSec 754
Ámbito de IPSec 755
Asociaciones de seguridad 755
Cabecera de autenticación 756
Encapsulado de la carga útil de seguridad 758

21.7. Lecturas y sitios web recomendados 759

21.8. Términos clave, cuestiones de repaso y ejercicios 759
Términos clave 759
Cuestiones de repaso 760
Ejercicios .....

Capítulo 22. Aplicaciones distribuidas 763

22.1. Correo electrónico-SMTP y MIME 764
Protocolo simple de transferencia de correo (SMTP) 765
Extensiones multipropósito de correo electrónico (MIME) 772

22.2. Protocolo de transferencia de hipertexto (HTTP) 780
Descripción general de HTTP 780
Mensajes 784
Mensajes de solicitud 786
Mensajes de respuesta 790
Entidades 792

22.3. Gestión de red-SNMP 793
Sistemas de gestión de red 794
Protocolo simple de gestión de red, versión 1 (SNMPv1) 794
Protocolo simple de gestión de red, versión 2 (SNMPv2) 798
Protocolo simple de gestión de red, versión 3 (SNMPv3) 803

22.4. Lecturas y sitios web recomendados 804

22.5. Términos clave, cuestiones de repaso y ejercicios 805
Términos clave 805
Cuestiones de repaso 805
Ejercicios 805

Apéndice A. RFC citados en este libro 807

Apéndice B. Análisis de Fourier 809

B.1. Desarrollo en serie de Fourier para señales periódicas 809

B.2. Transformada de Fourier para señales no periódicas 810
Densidad de potencia espectral y ancho de banda 810

B.3. Lecturas recomendadas 813

Apéndice C. Programación de *sockets* 815

Apéndice D. Proyectos para la enseñanza de comunicaciones de datos y redes de computadores 817
D.1. Proyectos de simulación 817
D.2. Modelado de rendimiento 818
D.3. Proyectos de investigación 819
D.4. Trabajos de lecturas y elaboración de informes 819
Glosario 821
Bibliografía 831
Índice alfabético 839

Prólogo

OBJETIVOS

Este libro intenta proporcionar una visión unificada del amplio campo que comprenden las comunicaciones y redes de computadores. La organización del libro refleja un intento de estructurar este vasto campo en partes comprensibles y de construir, poco a poco, una visión panorámica de su estado actual. El libro destaca principios básicos y temas de importancia fundamental que conciernen a la tecnología y arquitectura de esta área, proporcionando, además, una discusión detallada de temas de vanguardia.

Para unificar la discusión, se utilizan los siguientes criterios básicos:

- **Principios.** A pesar de que el alcance de este libro es muy amplio, hay varios principios básicos que aparecen repetidamente como temas y que unifican el campo. Por ejemplo, la multiplexación, el control de flujo y el control de errores. El libro destaca estos principios y contrasta su aplicación en áreas específicas de la tecnología.
- **Aproximaciones de diseño.** El libro examina distintos enfoques alternativos para satisfacer especificaciones concretas de comunicaciones.
- **Normalizaciones.** Las normalizaciones han llegado a asumir un papel en el campo importante y creciente e, incluso, dominante. Para entender el estado actual de la tecnología, y su evolución futura, se requiere una discusión amplia de las normalizaciones relacionadas con el campo.

ESTRUCTURA DEL TEXTO

El libro se encuentra estructurado en cinco partes[1]:

- I. **Introducción:** incluye una introducción al abanico de los distintos temas abordados en el libro. Además, esta parte incluye una discusión sobre protocolos OSI y el conjunto de protocolos TCP/IP.

[1] *N. del editor:* en la edición inglesa resulta evidente que, por error, se omite la relación de partes del libro. Las relacionadas aquí están extraídas de la sexta edición, ya que son las mismas.

- II. **Comunicaciones de datos:** ésta parte se refiere principalmente al intercambio de datos entre dos dispositivos directamente conectados. Dentro de esta situación restrictiva, se examinan los aspectos clave de la transmisión, interfaces, control de enlace y multiplexación.

- III. **Redes de área amplia:** ésta parte examina los mecanismos internos y la tecnología que se han desarrollado para admitir voz, datos y comunicaciones multimedia en redes que cubren grandes distancias. Se examinan las tecnologías tradicionales de conmutación de paquetes y conmutación de circuitos, así como la más reciente de ATM. Un capítulo independiente se dedica a los temas de control de congestión.

- IV. **Redes de área local:** ésta parte explora las tecnologías y arquitecturas que se han desarrollado para la interconexión de redes en distancias más cortas. Se analizan los medios de transmisión, las topologías y los protocolos de control de acceso al medio, que son los ingredientes clave del diseño LAN, y se estudian sistemas específicos LAN normalizados.

- V. **Protocolos de red:** ésta parte explora tanto los principios arquitectónicos como los mecanismos requeridos para el intercambio de datos entre computadores, estaciones de trabajo, servidores y otros sistemas de procesamiento de datos. Gran parte del material de esta sección se refiere al conjunto de protocolos TCP/IP.

Adicionalmente, el libro incluye un extenso glosario, una lista de los acrónimos más frecuentemente usados y una bibliografía. Cada capítulo incluye ejercicios y sugerencias de lecturas complementarias.

El libro va dirigido a una audiencia tanto académica como profesional. Para los profesionales interesados en este campo, el libro sirve como obra de referencia básica y es adecuado para autoestudio. Como libro de texto, puede usarse para un curso de uno o dos semestres. Comprende material descrito en el curso de «Redes de comunicaciones entre computadores» del *ACM/IEEE Computing Curricula 2001*. Los capítulos y partes del libro son suficientemente modulares como para proporcionar gran flexibilidad en la estructuración de cursos. A continuación, se proporcionan algunas sugerencias para diseñar un curso:

- **Fundamentos de comunicaciones de datos:** Partes I (introducción) y II (comunicaciones de datos) y Capítulos 10 y 11 (conmutación de circuitos, conmutación de paquetes y ATM).

- **Redes de comunicaciones:** si el estudiante tiene conocimientos básicos de comunicaciones de datos, este curso podría comprender: Parte I (introducción), Parte III (WAN) y Parte IV (LAN).

- **Redes de computadores:** si el estudiante dispone de conocimientos básicos de comunicaciones de datos, entonces este curso podría incluir: Parte I (introducción), Capítulos 6 y 7 (interfaces de comunicaciones de datos y control de enlace de datos) y la Parte V (protocolos).

Además, es posible un curso más profundo, comprendiendo la totalidad del libro salvo ciertos capítulos que no son esenciales en una primera lectura. Los capítulos que podrían ser opcionales son: los Capítulos 3 (transmisión de datos) y 4 (medios de transmisión), si el alumno tiene unos conocimientos básicos sobre estos temas; el Capítulo 8 (multiplexación); el Capítulo 9 (espectro expandido); los Capítulos 12 a 14 (encaminamiento, control de congestión y redes celulares); el Capítulo 18 (interconexión de redes) y el Capítulo 21 (seguridad en redes).

SERVICIOS INTERNET PARA PROFESORES Y ESTUDIANTES

Existe un sitio web para este libro que proporciona ayuda para los estudiantes y profesores. El sitio incluye enlaces a otros lugares relevantes, transparencias con las figuras del libro e información para suscribirse a una lista de distribución de correo de Internet con información sobre este libro. La dirección web de la página es williamstallings.com/DCC/DCC7e.html (*véase* la sección «Página web para comunicaciones de datos y redes de computadores» que precede a la tabla de contenidos para mayor información). También se ha establecido una lista de distribución de Internet para que los profesores que usen este libro puedan intercambiar información, sugerencias y preguntas entre ellos y con el autor. Tan pronto como se detecten errores tipográficos o de otro tipo se incluirá una fe de erratas del libro en williamstallings.com.

PROYECTOS PARA LA ENSEÑANZA DE COMUNICACIONES Y REDES DE COMPUTADORES

Para muchos profesores, un componente importante de un curso de comunicaciones y redes de computadores es un proyecto o conjunto de proyectos con los que el estudiante vaya adquiriendo experiencia práctica para reforzar los conceptos del texto. Este libro proporciona un grado incomparable de apoyo, ya que incluye una sección de proyectos en el curso. El manual del profesor no sólo incluye una guía de cómo asignar y estructurar los proyectos, sino también un conjunto de proyectos propuestos que abarcan un amplio rango de la materia de este texto, entre los que se encuentran proyectos de investigación, proyectos de simulación, proyectos de modelado analítico y asignación de informes de recopilación bibliográfica. Para más detalles puede verse el Apéndice D.

PROGRAMACIÓN DE SOCKETS

El libro incluye una breve descripción de los *sockets* (Apéndice C), junto con una descripción más detallada en el sitio web del libro. El manual del profesor incluye un conjunto de proyectos de programación. La programación de *sockets* es un aspecto «sencillo» que puede resultar en proyectos prácticos altamente satisfactorios para los alumnos.

NOVEDADES EN LA SÉPTIMA EDICIÓN

La séptima edición ve la luz menos de 4 años después de la publicación de la sexta edición. Durante este tiempo, el ritmo de los cambios continúa sin disminuir. En esta nueva edición, he tratado de captar estas innovaciones, manteniendo a la vez una visión amplia y comprensible del campo completo. Para realizar este proceso de revisión, la sexta edición fue ampliamente revisada por diversos profesores que imparten esta materia. El resultado es que, en muchos sitios, la narración ha sido clarificada y ajustada, así como mejoradas las ilustraciones. También se han añadido nuevos «problemas de campo».

Más allá de estos refinamientos para mejorar la pedagogía y el uso cómodo del libro, se han introducido algunos cambios relevantes a lo largo del mismo. Cada capítulo ha sido revisado, se han añadido nuevos capítulos y se ha modificado la organización global del libro. Los cambios más notables son los siguientes:

- **Comunicaciones inalámbricas y redes.** Se ha incrementado significativamente la cantidad de material dedicado a las comunicaciones, redes y estándares inalámbricos. El libro dedica

ahora un capítulo a la tecnología de espectro expandido, otro a las redes celulares inalámbricas y otro a las LAN inalámbricas.

- **Ethernet Gigabit.** La discusión sobre Ethernet Gigabit ha sido actualizada y se ha añadido una introducción a Ethernet a 10 Gbps.
- **Servicios diferenciados**. Se han realizado desarrollos sustanciales desde la publicación de la sexta edición en mejoras a Internet para dar soporte a una variedad de tráfico multimedia y sensible a retardos. El desarrollo más importante, y quizá el vehículo más importante para proporcionar QoS a las redes basadas en IP, lo constituyen los servicios diferenciados (DS, *Differentiated services*). Esta edición proporciona un minucioso estudio de DS.
- **Tasa de tramas garantizada** (GFR, *Guaranteed Frame Rate*). Desde la sexta edición, se ha estandarizado un nuevo servicio ATM, denominado GFR. GFR ha sido específicamente diseñado para las subredes troncales IP. Esta edición proporciona una explicación de GFR y examina los mecanismos subyacentes en el servicio GFR.
- **Conmutación de etiqueta multiprotocolo** (MPLS, *Multiprotocol Label Switching*). MPLS ha emergido como una tecnología de gran importancia en Internet, siendo cubierta en esta edición.
- **Detalles TCP/IP.** Se ha añadido un nuevo capítulo básico sobre TCP e IP, reuniendo material diseminado en la sexta edición. Este material es vital para comprender la QoS y los aspectos de rendimiento de las redes basadas en IP.

Además, a través del libro, la mayoría de los tópicos han sido actualizados para reflejar los desarrollos en normalizaciones y tecnología que han tenido lugar desde la publicación de la quinta edición.

AGRADECIMIENTOS

Esta nueva edición se ha beneficiado de la revisión de una serie de personas que han aportado su tiempo y conocimientos. Las siguientes personas han revisado todo o gran parte del manuscrito: Michael J. Donahoo (Universidad de Baylor), Gary Harbin (Universidad Estatal de Montana), Larry Owens (Universidad Estatal de California en Fresno), S. Hossein Hosseini (U. de Wisconsin-Milwaukee) y el Dr. Charles Baker (Universidad Metodista Sureña).

Gracias también a las muchas personas que realizaron detalladas revisiones técnicas de un único capítulo: Dave Tweed, Bruce Lane, Denis McMahon, Charles Freund, Paul Hoadley, Stephen Ma, Sandeep Subramaniam, Dragan Cvetkovic, Fernando Gont, Neil Giles, Rajes Thundil y Rick Jones.

Finalmente, me gustaría dar las gracias a los responsables de la publicación de este libro, todos los cuales realizaron su trabajo, como es habitual, de forma excelente. Esto incluye al personal de Prentice Hall, particularmente a mi editor, Alan Apt, su asistente Patrick Lindner y la directora de producción, Rose Kernan. También, a Jake Warde, de Warde Publishers, que gestionó los suplementos y revisiones, y a Patricia M. Daly, que realizó la maquetación.

CAPÍTULO 0

Guía del lector

0.1. Resumen del texto

0.2. Internet y recursos web
Sitios web relacionados con el texto
Otros sitios web
Grupos de noticias USENET

0.3. Estándares

Este libro, y el correspondiente sitio web asociado, tienen por objeto de estudio una gran cantidad de materia. A continuación, se proporciona al lector información básica sobre los contenidos considerados a lo largo del texto.

0.1. RESUMEN DEL TEXTO

El libro se ha organizado en las cinco partes siguientes:

Parte I. Visión general: presenta una introducción al extenso conjunto de temas abordados en el texto. Además, esta parte incluye una descripción general de las comunicaciones de datos y las redes, así como una discusión de los protocolos OSI y de la familia TCP/IP.

Parte II. Comunicaciones de datos: esta parte está relacionada fundamentalmente con el intercambio de datos entre dos dispositivos conectados directamente entre sí. Dentro de este contexto restringido, se estudian los conceptos clave de transmisión, interfaces, control del enlace y multiplexación.

Parte III. Redes de área amplia: en esta parte se estudian los mecanismos internos y las interfaces entre el usuario y la red, desarrollados para transmitir voz, datos y comunicaciones multimedia usando redes de larga distancia. Se examinan las tecnologías tradicionales de conmutación de paquetes y de circuitos, así como las tecnologías más recientes de ATM y WAN inalámbricas. Se dedica un capítulo independiente a las cuestiones relacionadas con el control de la congestión.

Parte IV. Redes de área local: esta parte explora las tecnologías y arquitecturas desarrolladas para las redes de distancias más cortas. Se analizan los medios de transmisión, las topologías y los protocolos para el control del acceso al medio, los cuales son los ingredientes básicos del diseño LAN. Igualmente, se estudian sistemas LAN concretos que han sido normalizados.

Parte V. Arquitectura de comunicaciones y protocolos: en esta parte se exploran tanto los principios arquitectónicos como los mecanismos necesarios para el intercambio de datos entre computadores, estaciones de trabajo, servidores y otros dispositivos de procesamiento. La mayor parte del material de este bloque está relacionado con la familia TCP/IP.

Al principio de cada parte, se proporciona un resumen más detallado, capítulo a capítulo, de los contenidos abordados.

0.2. INTERNET Y RECURSOS WEB

Hay una serie de recursos disponibles en Internet y en la Web para complementar este texto que pueden ayudar al lector a estar actualizado respecto a los desarrollos llevados a cabo en este campo.

SITIOS WEB RELACIONADOS CON EL TEXTO

Se ha habilitado una página web para este libro, disponible en WilliamStallings.com/DCC/DCC7e.html. Para obtener una descripción detallada de su contenido *véase* el esquema de dos páginas mostrado al principio del libro.

Tan pronto como se detecten erratas tipográficas o cualquier otra clase de errores, se publicarán en el mencionado sitio web. Por favor, comuniquen cualquier tipo de error detectado. En WilliamStallings.com se pueden encontrar listas de erratas para otros libros del autor, así como ofertas para su adquisición.

El autor también mantiene un sitio web con recursos para estudiantes de computación en WilliamStallings.com/StudentSupport.html. El objetivo es proporcionar documentos, información y enlaces para los estudiantes de computación. Los enlaces se han estructurado en cuatro categorías:

- **Matemáticas:** incluye un repaso básico de matemáticas, una introducción a la teoría de colas, una introducción a los sistemas binario y decimal, así como enlaces a muchos sitios web relacionados con matemáticas.
- **CÓMO (*How-to*):** consejos y directrices para resolver problemas, escribir informes técnicos y preparar presentaciones técnicas.
- **Recursos para investigación:** enlaces a colecciones de artículos, informes técnicos y bibliografías relevantes.
- **Miscelánea:** Varios documentos y enlaces de utilidad.

OTROS SITIOS WEB

Hay una cantidad enorme de sitios web con información relacionada con los temas tratados en el libro. En los capítulos siguientes se pueden encontrar referencias de sitios web específicos en cada una de las secciones «Lecturas recomendadas». Debido a la tendencia que tienen las URL de cambiar frecuentemente, no han sido incluidas en este libro. Todos los sitios web citados a lo largo del libro pueden ser explorados a través de los correspondientes enlaces que se han habilitado en la página web del libro.

Las siguientes páginas web son de interés general y están relacionadas con las comunicaciones y redes de computadores:

- **El mundo de las redes:** información y enlaces a recursos sobre comunicaciones de datos y redes.
- **IETF:** mantiene archivos relacionados con Internet y sobre las actividades de la IETF. Incluye una biblioteca de RFC y de borradores indexada por palabras clave, así como otros muchos documentos relacionados con Internet y sus protocolos asociados.
- **Fabricantes:** enlaces a miles de páginas web de fabricantes de hardware y software, así como un directorio telefónico de miles de empresas de computadores y redes.
- ***IEEE Communications Society*:** una buena forma de estar informado sobre congresos, publicaciones, etc.
- ***ACM Special Interest Group on Communications* (*SIGCOMM*):** una buena forma de estar informado sobre congresos, publicaciones, etc.
- **Unión Internacional de Telecomunicaciones:** contiene una lista de recomendaciones de la UIT-T, más información para la obtención de documentos de la UIT-T impresos o en CD-ROM.
- **Organización Internacional de Estandarización (ISO):** contiene una lista de normas ISO, más información sobre cómo obtener documentos ISO impresos o en CD-ROM.
- **CommWeb:** enlaces a fabricantes, tutoriales y otras informaciones de utilidad.

GRUPOS DE NOTICIAS USENET

Existe una serie de grupos de noticias USENET dedicados a aspectos relacionados con la comunicación de datos, las redes y los protocolos. Como en casi todos los otros grupos USENET, en estos grupos hay una alta relación ruido-señal. A pesar de esto, vale la pena comprobar si algo se ajusta a sus necesidades. Los grupos más relevantes son:

- **comp.dcom.lan, comp.dcom.lans.misc:** discusiones genéricas sobre LAN;
- **comp.dcom.lans.ethernet:** acerca de Ethernet, de sistemas similares y de las normas IEEE 802.3 CSMA/CD;
- **comp.std.wireless:** debates sobre redes inalámbricas incluyendo, entre otras, LAN inalámbricas;
- **comp.security.misc:** seguridad en computadores y cifrado;
- **comp.dcom.cell-relay:** sobre ATM y LAN ATM;
- **comp.dcom.frame-relay:** sobre redes *frame relay*;
- **comp.dcom.net-management:** debates sobre aplicaciones de gestión de red, protocolos y estándares;
- **comp.protocol.tcp-ip:** sobre la familia TCP/IP.

0.3. ESTÁNDARES

En la industria de las comunicaciones, desde hace tiempo, se aceptó la necesidad de los estándares para definir las características físicas, eléctricas y de procedimiento de los equipos de comunicación. En el pasado, este punto de vista no era compartido por la industria de los computadores. Mientras que los fabricantes de equipos de comunicación comprendieron que sus equipos deberían, en general, interconectarse y comunicarse con equipos desarrollados por terceros, los fabricantes de computadores han venido intentando monopolizar a sus clientes. La proliferación de diferentes computadores y la generalización del procesamiento distribuido han desencadenado una situación insostenible. Los computadores de diferentes fabricantes deben comunicarse entre sí y, es más, dada la evolución actual en la normalización de los protocolos, los clientes no admiten ya tener que desarrollar o adquirir software para adaptar protocolos de uso específico. Como consecuencia, en la actualidad la normalización se está imponiendo en todas las áreas tecnológicas consideradas en este libro.

Hay una serie de ventajas y desventajas en el proceso de estandarización. A continuación, se citan las más relevantes. Las principales ventajas son:

- La existencia de un estándar para un software o equipo dado asegura potencialmente un gran mercado. Esto estimula la producción masiva y, en algunos casos, el uso de integración a gran escala (LSI) o integración a muy gran escala (VLSI), reduciéndose así los costes.
- Un estándar permite que los productos de diferentes fabricantes se comuniquen, dotando al comprador de mayor flexibilidad en la selección y uso de los equipos.

Las principales desventajas son:

- Los estándares tienden a congelar la tecnología. Mientras que un estándar se desarrolla, se revisa y se adopta, se pueden haber desarrollado otras técnicas más eficaces.

- Hay muchos estándares para la misma función. Este problema en realidad no es atribuible a la estandarización en sí, sino a la forma en la que se hacen las cosas. Afortunadamente, en los últimos años las organizaciones para la definición de estándares han comenzado a cooperar más estrechamente. No obstante, todavía hay áreas donde coexisten varios estándares en conflicto.

A lo largo de este libro, se describen los estándares más importantes relacionados con las comunicaciones y los computadores. Se consideran tanto aquellos que en la actualidad están en uso, como los que están en fase de desarrollo. Para la promoción o desarrollo de estos estándares han participado decisivamente varias organizaciones. Las organizaciones más importantes de normalización (en este contexto) son las siguientes:

- **La Asociación Internet:** la Asociación Internet (ISOC, *Internet SOCiety*) es una asociación profesional formada por más de 150 organizaciones y 6.000 miembros individuales de más de 100 países. ISOC lidera el planteamiento de las cuestiones que afectan al futuro de Internet, a la vez que es el organismo en torno al cual se organizan los grupos responsables de la normalización en Internet. A ésta pertenecen, entre otros, el Comité de Arquitectura de Internet (IAB, *Internet Architecure Board*) y el Comité de Ingeniería de Internet (IETF, *Internet Engineering Task Force*). Todos los RFC y normas en Internet se desarrollan en estas organizaciones.
- **IEEE 802:** el Comité para las Normas 802 LAN/MAN de IEEE (*Institute of Electrical and Electronics Engineers*) desarrolla los estándares para las redes de área local y redes de área metropolitana. Los estándares más utilizados son los correspondientes a la familia Ethernet, *token ring*, LAN inalámbricas, interconexión con puentes y LAN virtuales con puentes.
- **UIT-T:** la Unión Internacional de Telecomunicaciones (UIT) es una organización internacional perteneciente a las Naciones Unidas en la que los gobiernos y el sector privado coordinan las redes y los servicios globales de telecomunicación. El Sector para la Normalización de las Telecomunicaciones (UIT-T) es uno de los tres sectores de la UIT. Su misión es la especificación de normas en el campo de las telecomunicaciones.
- **El Forum ATM:** el Forum ATM es una organización internacional sin ánimo de lucro cuyo objetivo es la promoción de los productos y servicios de ATM (*Asynchronous Transfer Mode*) mediante especificaciones interoperativas rápidamente convergentes. Además, el Forum promueve la cooperación industrial.
- **ISO:** La Organización Internacional de Estandarización (ISO[1], *International Organization for Standardization*) es una federación mundial de organismos nacionales de normalización de más de 140 países, uno por cada uno de los países pertenecientes. ISO es una organización no gubernamental que promueve el desarrollo de la normalización y actividades relacionadas con la intención de facilitar el intercambio internacional de bienes y servicios, y el desarrollo de la cooperación en los ámbitos intelectual, científico, tecnológico y económico. El trabajo de ISO consiste en el establecimiento de acuerdos internacionales que se publican como Normas Internacionales.

La web correspondiente a este texto contiene un documento con información más detallada acerca de estas organizaciones.

[1] ISO no es en realidad el acrónimo (en su lugar debería ser literalmente IOS), sino una palabra derivada de la griega «isos», que significa *igual*.

PARTE I

DESCRIPCIÓN GENERAL

CUESTIONES DE LA PARTE I

El objetivo de la Parte I es definir los conceptos básicos, a la vez que especificar el contexto general en el que se desarrollará el resto del libro. En este capítulo se presenta un amplio espectro de cuestiones relacionadas con el campo de las redes y la transmisión de datos, además, se presentan los conceptos fundamentales relacionados con los protocolos y sus arquitecturas.

ESQUEMA DE LA PARTE I

CAPÍTULO 1. INTRODUCCIÓN A LAS COMUNICACIONES DE DATOS Y REDES

El Capítulo 1 proporciona una descripción general de los contenidos abordados en las Partes II, III y IV del texto; en él se consideran todos los temas que se estudiarán posteriormente. Esencialmente, en el libro se estudian cuatro conceptos: las comunicaciones de datos a través del enlace de transmisión, las redes de área amplia, las redes de área local, y los protocolos y la arquitectura TCP/IP. El Capítulo 1 es una introducción a los tres primeros conceptos mencionados.

CAPÍTULO 2. ARQUITECTURA DE PROTOCOLOS

En el Capítulo 2 se estudia el concepto de arquitectura de protocolos. Este Capítulo se puede leer inmediatamente después del Capítulo 1, o bien se puede posponer hasta antes del comienzo de las Partes III, IV o V.

Tras una introducción general, en este capítulo se estudian las dos arquitecturas más importantes: el modelo de Interconexión de Sistemas Abiertos (OSI, *Open System Interconnection*) y el modelo TCP/IP. Aunque el modelo OSI se utiliza habitualmente como referencia para introducir los conceptos, la familia de protocolos TCP/IP es, con diferencia, la base de la mayoría de los productos comerciales. Ésta es la razón que justifica su consideración en la Parte V del presente texto.

CAPÍTULO 1

Introducción a las comunicaciones de datos y redes

1.1. Un modelo para las comunicaciones

1.2. Comunicaciones de datos

1.3. Redes de transmisión de datos
Redes de área amplia
Redes de área local
Redes inalámbricas
Redes de área metropolitana

1.4. Un ejemplo de configuración

CUESTIONES BÁSICAS

- El objetivo de este texto es amplio y abarca tres grandes áreas: comunicaciones, redes y protocolos. Las dos primeras se presentan en este capítulo.
- El estudio de las comunicaciones aborda la transmisión de señales de forma tal que sea eficaz y segura. Entre otros aspectos, se estudiarán la transmisión y codificación de señales, los medios de transmisión, las interfaces, el control del enlace de datos y la multiplexación.
- En el estudio de las redes se abordará tanto la tecnología como los aspectos relacionados con las arquitecturas de redes de comunicación utilizadas para la interconexión de dispositivos. Esta materia se divide normalmente en redes de área local (LAN) y redes de área amplia (WAN).

En torno a los años 1970 y 1980 se produjo una sinergia entre los campos de los computadores y las comunicaciones que desencadenó un cambio drástico en las tecnologías, productos y en las propias empresas que, desde entonces, se dedican conjuntamente a los sectores de los computadores y de las comunicaciones. La revolución experimentada en el sector de los computadores y las comunicaciones ha producido los siguientes hechos significativos:

- No hay grandes diferencias entre el procesamiento de datos (los computadores) y las comunicaciones de datos (la transmisión y los sistemas de conmutación).
- No hay diferencias fundamentales entre la transmisión de datos, de voz o de vídeo.
- Las fronteras entre computadores monoprocesador o multiprocesador, así como las existentes entre las redes de área local, metropolitanas y de área amplia, se han difuminado.
- Un efecto de esta tendencia ha sido el creciente solapamiento que se puede observar entre las industrias de las comunicaciones y de los computadores, desde la fabricación de componentes hasta la integración de sistemas. Otro resultado es el desarrollo de sistemas integrados que transmiten y procesan todo tipo de datos e información. Las organizaciones de normalización, tanto técnicas como tecnológicas, tienden hacia sistemas públicos integrados que hagan accesibles virtualmente todos los datos y fuentes de información de manera fácil y uniforme a escala mundial.
- El objetivo fundamental de este texto es proporcionar una visión unificada del vasto campo de las comunicaciones de datos y los computadores. La organización del libro refleja un intento de dividir esta extensa materia en partes coherentes, proporcionando a la vez una visión de su estado actual. Este capítulo introductorio comienza presentando un modelo general para las comunicaciones. Posteriormente, se presentan de forma sucinta las Partes II a IV. En el Capítulo 2 se resume la Parte V.

1.1. UN MODELO PARA LAS COMUNICACIONES

Comenzaremos nuestro estudio considerando el modelo sencillo de sistema de comunicación mostrado en la Figura 1.1a, en la que se propone un diagrama de bloques.

El objetivo principal de todo sistema de comunicaciones es intercambiar información entre dos entidades. La Figura 1.1b muestra un ejemplo particular de comunicación entre una estación de

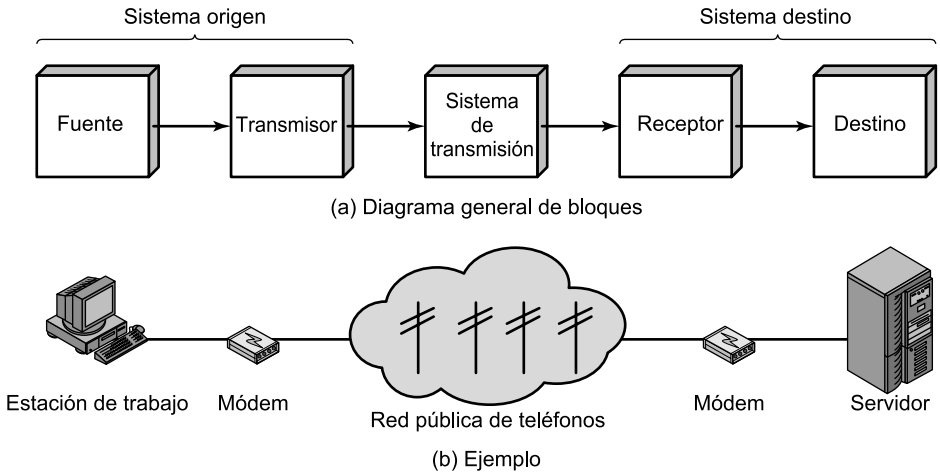


Figura 1.1. Modelo simplificado para las comunicaciones.

trabajo y un servidor a través de una red telefónica pública. Otro posible ejemplo consiste en el intercambio de señales de voz entre dos teléfonos a través de la misma red anterior. Los elementos clave en este modelo son los siguientes:

- **La fuente.** Este dispositivo genera los datos a transmitir. Ejemplos de fuentes pueden ser un teléfono o un computador personal.
- **El transmisor.** Normalmente los datos generados por la fuente no se transmiten directamente tal y como son generados. Al contrario, el transmisor transforma y codifica la información, generando señales electromagnéticas susceptibles de ser transmitidas a través de algún sistema de transmisión. Por ejemplo, un módem convierte las cadenas de bits generadas por un computador personal y las transforma en señales analógicas que pueden ser transmitidas a través de la red de telefonía.
- **El sistema de transmisión.** Puede ser desde una sencilla línea de transmisión hasta una compleja red que conecte a la fuente con el destino.
- **El receptor.** El receptor acepta la señal proveniente del sistema de transmisión y la transforma de tal manera que pueda ser manejada por el dispositivo de destino. Por ejemplo, un módem captará la señal analógica de la red o línea de transmisión y la convertirá en una cadena de bits.
- **El destino.** Toma los datos del receptor.

Aunque el modelo presentado pueda parecer aparentemente sencillo, en realidad implica una gran complejidad. Para hacerse una idea de la magnitud de ella, la Tabla 1.1 lista algunas de las tareas claves que se deben realizar en un sistema de comunicaciones. Esta relación es un tanto arbitraria ya que se podrían añadir elementos, mezclar ítems, etc; es más, algunos elementos representan tareas que se realizan en diferentes «niveles» del sistema. No obstante, la lista tal y como está es representativa del objeto de estudio de este texto.

El primer ítem, denominado **utilización del sistema de transmisión**, se refiere a la necesidad de hacer un uso eficaz de los recursos utilizados en la transmisión, los cuales se suelen compartir habitualmente entre una serie de dispositivos de comunicación. La capacidad total del medio de transmisión se reparte entre los distintos usuarios haciendo uso de técnicas denominadas de

TABLA 1.1. Tareas en los sistemas de comunicación.

Utilización del sistema de transmisión	Direccionamiento
Implementación de la interfaz	Encaminamiento
Generación de la señal	Recuperación
Sincronización	Formato de mensajes
Gestión del intercambio	Seguridad
Detección y corrección de errores	Gestión de red
Control de flujo	

multiplexación. Además, puede que se necesiten técnicas de control de congestión para garantizar que el sistema no se sature por una demanda excesiva de servicios de transmisión.

Para que un dispositivo pueda transmitir información tendrá que hacerlo a través de la **interfaz** con el medio de transmisión. Todas las técnicas de transmisión presentadas en este libro dependen, en última instancia, de la utilización de señales electromagnéticas que se transmitirán a través del medio. Así, una vez que la interfaz está establecida, será necesaria la **generación de la señal**. Las características de la señal, como la forma y la intensidad, deben ser tales que permitan 1) que la señal se propague a través del medio de transmisión y que 2) se interprete en el receptor como datos.

Las señales se deben generar no sólo considerando que deben cumplir los requisitos del sistema de transmisión y del receptor, sino que también deben permitir alguna forma de **sincronizar** el receptor y el emisor. El receptor debe ser capaz de determinar cuándo comienza y cuándo acaba la señal recibida. Igualmente, deberá conocer la duración de cada elemento de señal.

Además de las cuestiones básicas referentes a la naturaleza y temporización de las señales, se necesitará verificar un conjunto de requisitos que se pueden englobar bajo el término **gestión del intercambio**. Si se necesita intercambiar datos durante un periodo de tiempo, las dos partes deben cooperar. Por ejemplo, para los dos elementos que intervienen en una conversación de telefonía (emisor y receptor), uno de ellos deberá marcar el número del otro, dando lugar a una serie de señales que harán que el otro teléfono suene. En este ejemplo el receptor establecerá la llamada descolgando el auricular. En los dispositivos para el procesamiento de datos se necesitarán ciertas convenciones además del simple hecho de establecer la conexión. Por ejemplo, se deberá establecer si ambos dispositivos pueden transmitir simultáneamente o deben hacerlo por turnos, se deberá decidir la cantidad y el formato de los datos que se transmiten cada vez y se deberá especificar qué hacer en caso de que se den ciertas contingencias, como por ejemplo la detección de un error.

Los dos ítems siguientes podrían considerarse dentro de la gestión del intercambio, pero, debido a su importancia, se consideran por separado. En todos los sistemas de comunicación es posible que aparezcan errores; ya que la señal transmitida se distorsiona siempre (por poco que sea) antes de alcanzar su destino. Por tanto, en circunstancias donde no se puedan tolerar, se necesitarán procedimientos para la **detección y corrección de errores.** Éste es habitualmente el caso en los sistemas para el procesamiento de datos, así por ejemplo, si se transfiere un fichero desde un computador a otro, no sería aceptable que el contenido del fichero se modificara accidentalmente. Por otra parte, para evitar que la fuente no sature el destino transmitiendo datos más rápidamente de lo que el receptor pueda procesar y absorber, se necesitan una serie de procedimientos denominados **control de flujo**.

Conceptos relacionados pero distintos a los anteriores son el **direccionamiento** y el **encaminamiento**. Cuando cierto recurso de transmisión se comparte con más de dos dispositivos, el sistema fuente deberá, de alguna manera, indicar la identidad del destino. El sistema de transmisión deberá

garantizar que ese destino, y sólo ése, recibe los datos. Es más, el sistema de transmisión puede ser una red en la que exista la posibilidad de usar más de un camino para alcanzar el destino; en este caso se necesitará, por tanto, la elección de una de entre las posibles rutas.

La **recuperación** es un concepto distinto a la corrección de errores. En ciertas situaciones en las que el intercambio de información, por ejemplo una transacción de una base de datos o la transferencia de un fichero, se vea interrumpido por algún fallo, se necesitará un mecanismo de recuperación. El objetivo será, pues, o bien ser capaz de continuar transmitiendo desde donde se produjo la interrupción, o, al menos, recuperar el estado en el que se encontraban los sistemas involucrados antes de comenzar el intercambio.

El **formato de mensajes** está relacionado con el acuerdo que debe existir entre las dos partes respecto al formato de los datos intercambiados, como por ejemplo, el código binario usado para representar los caracteres.

Además, frecuentemente es necesario dotar al sistema de algunas medidas de **seguridad**. El emisor puede querer asegurarse de que sólo el destino deseado reciba los datos. Igualmente, el receptor querrá estar seguro de que los datos recibidos no se han alterado en la transmisión y que dichos datos realmente provienen del supuesto emisor.

Por último, todo el sistema de comunicación es lo suficientemente complejo como para ser diseñado y utilizado sin más, es decir, se necesitan funcionalidades de **gestión de red** para configurar el sistema, monitorizar su estado, reaccionar ante fallos y sobrecargas y planificar con acierto los crecimientos futuros.

Como se ha visto, de la aproximación simplista de partida hemos formulado una lista más extensa y elaborada de tareas involucradas en todo el proceso de la comunicación. A lo largo de este libro esta lista se estudiará en profundidad, describiendo todo el conjunto de tareas y actividades que pueden englobarse genéricamente bajo los términos comunicación de datos y redes de computadores.

1.2. COMUNICACIONES DE DATOS

Tras el estudio de la Parte I, el libro se ha estructurado en cuatro partes adicionales. La segunda parte aborda, fundamentalmente, los temas relacionados con las funciones de comunicación, centrándose en la transmisión de señales de una forma fiable y eficiente. Intencionadamente dicha Parte II se ha titulado «Comunicaciones de datos», aunque con ese término se alude a algunos, o incluso a todos los tópicos de las restantes partes (de la III a la V).

Para explicar todos los conceptos abordados en la Parte II, la Figura 1.2 muestra una perspectiva novedosa del modelo tradicional para las comunicaciones de la Figura 1.1a. Dicha figura se explica a continuación, paso a paso, con la ayuda de un ejemplo: la aplicación de correo electrónico.

Supóngase que tanto el dispositivo de entrada como el transmisor están en un computador personal. Y que, por ejemplo, el usuario de dicho PC desea enviar el mensaje m a otro. El usuario activa la aplicación de correo en el PC y compone el mensaje con el teclado (dispositivo de entrada). La cadena de caracteres se almacenará temporalmente en la memoria principal como una secuencia de bits (g). El computador se conecta a algún medio de transmisión, por ejemplo una red local o una línea de telefonía, a través de un dispositivo de E/S (transmisor), como por ejemplo un transceptor en una red local o un módem. Los datos de entrada se transfieren al transmisor como una secuencia de niveles de tensión [$g(t)$] que representan los bits en algún tipo de bus de comunicaciones o

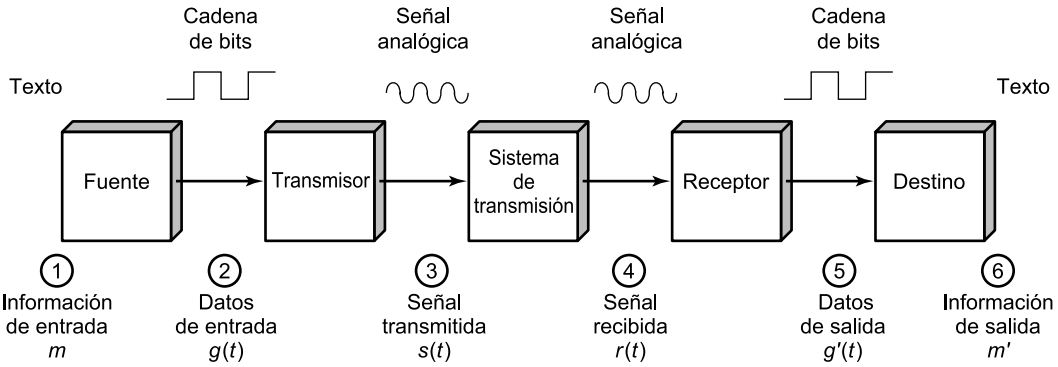


Figura 1.2. Modelo simplificado para las comunicaciones de datos.

cable. El transmisor se conecta directamente al medio y convierte la cadena [$g(t)$] en la señal a transmitir [$s(t)$]. En el Capítulo 5 se describirán las distintas alternativas para esta conversión.

Al transmitir $s(t)$ a través del medio, antes de llegar al receptor, aparecerán una serie de dificultades que se estudiarán en el Capítulo 3. Por tanto, la señal recibida $r(t)$ puede diferir de alguna manera de la transmitida $s(t)$. El receptor intentará estimar la señal original $s(t)$, a partir de la señal $r(t)$ y de su conocimiento acerca del medio, obteniendo una secuencia de bits $g'(t)$. Estos bits se envían al computador de salida, donde se almacenan temporalmente en memoria como un bloque de bits g'. En muchos casos, el destino intentará determinar si ha ocurrido un error y, en su caso, cooperar con el origen para, eventualmente, conseguir el bloque de datos completo y sin errores. Los datos, finalmente, se presentan al usuario a través del dispositivo de salida, que por ejemplo puede ser la impresora o la pantalla de su terminal. El mensaje recibido por el usuario (m') será normalmente una copia exacta del mensaje original (m).

Consideremos ahora una conversación usando el teléfono. En este caso, la entrada al teléfono es un mensaje (m) consistente en una onda sonora. Dicha onda se convierte en el teléfono en señales eléctricas con los mismos componentes en frecuencia. Estas señales se transmiten sin modificación a través de la línea telefónica. Por tanto, la señal de entrada $g(t)$ y la señal transmitida $s(t)$ son idénticas. La señal $s(t)$ sufrirá algún tipo de distorsión a través del medio, de tal manera que $r(t)$ no será idéntica a $s(t)$. No obstante, la señal $r(t)$ se convierte recuperando una onda sonora, sin aplicar ningún tipo de corrección o mejora de la calidad. Por tanto, m' no será una réplica exacta de m. Sin embargo, el mensaje sonoro recibido es normalmente comprensible por el receptor.

En el ejemplo anterior no se han considerado otros aspectos fundamentales en las comunicaciones de datos, como lo son las técnicas de control del enlace, necesarias para regular el flujo de datos, o como la detección y corrección de errores. Tampoco se han considerado las técnicas de multiplexación, necesarias para conseguir una utilización eficaz del medio de transmisión. Todos estos aspectos se estudian en la Parte II.

1.3. REDES DE TRANSMISIÓN DE DATOS

A veces no es práctico que dos dispositivos de comunicaciones se conecten directamente mediante un enlace punto a punto. Esto es debido a alguna (o a las dos) de las siguientes circunstancias:

- Los dispositivos están muy alejados. En este caso no estaría justificado, por ejemplo, utilizar un enlace dedicado entre dos dispositivos que puedan estar separados por miles de kilómetros.

- Hay un conjunto de dispositivos que necesitan conectarse entre ellos en instantes de tiempo diferentes. Un ejemplo de esta necesidad es la red de teléfonos mundial o el conjunto de computadores pertenecientes a una compañía. Salvo el caso de que el número de dispositivos sea pequeño, no es práctico utilizar un enlace entre cada dos.

La solución a este problema es conectar cada dispositivo a una red de comunicación. Para clasificar las redes tradicionalmente se consideran dos grandes categorías: las redes de área amplia (WAN, *Wide Area Networks*) y las redes de área local (LAN, *Local Area Networks*). Las diferencias entre estas dos categorías son cada vez más difusas, tanto en términos tecnológicos como de posibles aplicaciones; no obstante, es una forma natural y didáctica de organizar su estudio, por lo que aquí se adoptará dicha clasificación.

REDES DE ÁREA AMPLIA

Generalmente, se considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan, al menos parcialmente, circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Generalmente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo los situados en los contornos) no les concierne el contendido de los datos, al contrario, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

Tradicionalmente, las WAN se han implementado usando una de las dos tecnologías siguientes: conmutación de circuitos y conmutación de paquetes. Últimamente, se está empleando como solución la técnica de retransmisión de tramas (*frame relay*), así como las redes ATM.

Conmutación de circuitos

En las redes de conmutación de circuitos, para interconectar dos estaciones se establece un camino dedicado a través de los nodos de la red. El camino es una secuencia conectada de enlaces físicos entre nodos. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino dedicado tan rápido como se pueda. En cada nodo, los datos de entrada se encaminan o conmutan por el canal apropiado de salida sin retardos. El ejemplo más ilustrativo de la conmutación de circuitos es la red de telefonía.

Conmutación de paquetes

Un enfoque diferente al anterior es el adoptado en las redes de conmutación de paquetes. En este caso, no es necesario hacer una asignación a priori de recursos (capacidad de transmisión) en el camino (o sucesión de nodos). Por el contrario, los datos se envían en secuencias de pequeñas unidades llamadas paquetes. Cada paquete se pasa de nodo en nodo en la red siguiendo algún camino entre la estación origen y la destino. En cada nodo, el paquete se recibe completamente, se almacena durante un breve intervalo y posteriormente se retransmite al siguiente nodo. Las redes de conmutación de paquetes se usan fundamentalmente para las comunicaciones terminal-computador y computador-computador.

Retransmisión de tramas (*frame relay*)

La conmutación de paquetes se desarrolló en la época en la que los servicios de transmisión a larga distancia presentaban una tasa de error relativamente elevada, comparada con los servicios de los que se dispone actualmente. Por tanto, para compensar esos errores relativamente frecuentes, en los esquemas de conmutación de paquetes se realiza un esfuerzo considerable, que se traduce en añadir información redundante en cada paquete así como en la realización de un procesamiento extra, tanto en el destino final como en los nodos intermedios de conmutación, necesario para detectar los errores y, en su caso, corregirlos.

Ahora bien, con los modernos sistemas de telecomunicación de alta velocidad, este esfuerzo adicional es innecesario e incluso contraproducente. Es innecesario ya que la tasa de errores se ha reducido drásticamente y los escasos errores que aparecen se pueden tratar en el sistema final mediante dispositivos que operan por encima del nivel de la lógica dedicada a la conmutación de paquetes. A su vez, es contraproducente ya que los bits redundantes introducen un desaprovechamiento de parte de la capacidad proporcionada por la red.

La tecnología de retransmisión de tramas se ha desarrollado teniendo presente que las velocidades de transmisión disponibles en la actualidad son mayores, así como que las tasas de error actuales son menores. Mientras que las redes originales de conmutación de paquetes se diseñaron para ofrecer una velocidad de transmisión al usuario final de 64 kbps, las redes con retransmisión de tramas están diseñadas para operar eficazmente a velocidades de transmisión de usuario de hasta 2 Mbps. La clave para conseguir estas velocidades reside en eliminar la mayor parte de la información redundante usada para el control de errores y, en consecuencia, el procesamiento asociado.

ATM

El Modo de Transferencia Asíncrono (ATM, *Asynchronous Transfer Mode*), a veces denominado como modo de retransmisión de celdas (*cell relay*), es la culminación de todos los desarrollos en conmutación de circuitos y conmutación de paquetes. ATM se puede considerar como una evolución de la retransmisión de tramas. La diferencia más obvia entre retransmisión de tramas y ATM es que la primera usa paquetes de longitud variable, llamados «tramas», y ATM usa paquetes de longitud fija denominados «celdas». Al igual que en retransmisión de tramas, ATM introduce poca información adicional para el control de errores, confiando en la inherente robustez del medio de transmisión así como en la lógica adicional localizada en el sistema destino para detectar y corregir errores. Al utilizar paquetes de longitud fija, el esfuerzo adicional de procesamiento se reduce incluso todavía más que en retransmisión de tramas. El resultado es que ATM se ha diseñado para trabajar a velocidades de transmisión del orden de 10 a 100 Mbps, e incluso del orden de Gbps.

ATM se puede considerar, a su vez, como una evolución de la conmutación de circuitos. En la conmutación de circuitos se dispone solamente de circuitos a velocidad fija de transmisión entre los sistemas finales. ATM permite la definición de múltiples canales virtuales con velocidades de transmisión que se definen dinámicamente en el instante en el que se crea el canal virtual. Al utilizar celdas de tamaño fijo, ATM es tan eficaz que puede ofrecer un canal a velocidad de transmisión constante aunque esté usando una técnica de conmutación de paquetes. Por tanto, en este sentido, ATM es una generalización de la conmutación de circuitos en la que se ofrecen varios canales, en los que la velocidad de transmisión se fija dinámicamente para cada canal según las necesidades.

REDES DE ÁREA LOCAL

Al igual que las redes WAN, una LAN es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos. No obstante, hay algunas diferencias entre las LAN y las WAN que se enumeran a continuación:

1. La cobertura de una LAN es pequeña, generalmente un edificio o, a lo sumo, un conjunto de edificios próximos. Como se verá más adelante, esta diferencia en cuanto a la cobertura geográfica condicionará la solución técnica finalmente adoptada.
2. Es habitual que la LAN sea propiedad de la misma entidad propietaria de los dispositivos conectados a la red. En WAN, esto no es tan habitual o, al menos, una fracción significativa de recursos de la red son ajenos. Esto tiene dos implicaciones. La primera es que se debe cuidar mucho la elección de la LAN, ya que, evidentemente, lleva acarreada una inversión sustancial de capital (comparada con los gastos de conexión o alquiler de líneas en redes de área amplia) tanto en la adquisición como en el mantenimiento. Segunda, la responsabilidad de la gestión de la red local recae solamente en el usuario.
3. Por lo general, las velocidades de transmisión internas en una LAN son mucho mayores que en una WAN.

Para las LAN hay muy diversas configuraciones. De entre ellas, las más habituales son las LAN conmutadas y las LAN inalámbricas. Dentro de las conmutadas, las más populares son las LAN Ethernet, constituidas por un único conmutador, o, alternativamente, implementadas mediante un conjunto de conmutadores interconectados entre sí. Otro ejemplo muy relevante son las LAN ATM, caracterizadas por utilizar tecnología de red ATM en un entorno local. Por último, son también destacables las LAN con canal de fibra (*Fiber Channel*). En las LAN inalámbricas se utilizan diversos tipos de tecnologías de transmisión y distintos tipos de configuraciones. Las LAN se estudian en profundidad en la Parte IV.

REDES INALÁMBRICAS

Como ya se ha mencionado, las LAN inalámbricas son bastante habituales, fundamentalmente en entornos de oficinas. La tecnología inalámbrica es también muy utilizada en redes de área amplia de voz y datos. Las redes inalámbricas proporcionan ventajas evidentes en términos de movilidad y facilidad de instalación y configuración. Las redes WAN y LAN inalámbricas se estudian, respectivamente, en los Capítulos 14 y 17.

REDES DE ÁREA METROPOLITANA

Como el propio nombre sugiere, las MAN (*Metropolitan Area Network*) están entre las LAN y las WAN. El interés en las MAN ha surgido tras ponerse de manifiesto que las técnicas tradicionales de conmutación y conexión punto a punto usadas en WAN, pueden ser no adecuadas para las necesidades crecientes de ciertas organizaciones. Mientras que la retransmisión de tramas y ATM prometen satisfacer un amplio espectro de necesidades en cuanto a velocidades de transmisión, hay situaciones, tanto en redes privadas como públicas, que demandan gran capacidad a coste reducido en áreas relativamente grandes. Para tal fin se han implementado una serie de soluciones, como por ejemplo las redes inalámbricas o las extensiones metropolitanas de Ethernet.

El principal mercado para las MAN lo constituyen aquellos clientes que necesitan alta capacidad en un área metropolitana. Las MAN están concebidas para satisfacer estas necesidades de capacidad a un coste reducido y con una eficacia mayor que la que se obtendría mediante una compañía local de telefonía para un servicio equivalente.

1.4. UN EJEMPLO DE CONFIGURACIÓN

Para dar una idea de conjunto de los objetivos de las Partes II, III y IV del texto, en la Figura 1.3 se muestra un escenario de comunicación típico junto con los elementos constituyentes de una red de las usadas en la actualidad. En la esquina superior izquierda, se puede encontrar un usuario residencial conectado a Internet a través de un proveedor de acceso a Internet o, del inglés, ISP (*Internet Service Provider*) mediante algún tipo de conexión de abonado. Ejemplos habituales para esa conexión son la red pública de telefonía, para lo que el usuario necesitaría un módem (generalmente a 56 Kbps); una línea digital de abonado, DSL (*Digital Subscriber Line*), tecnología que proporciona un enlace de alta velocidad a través de líneas de telefonía mediante el uso de un

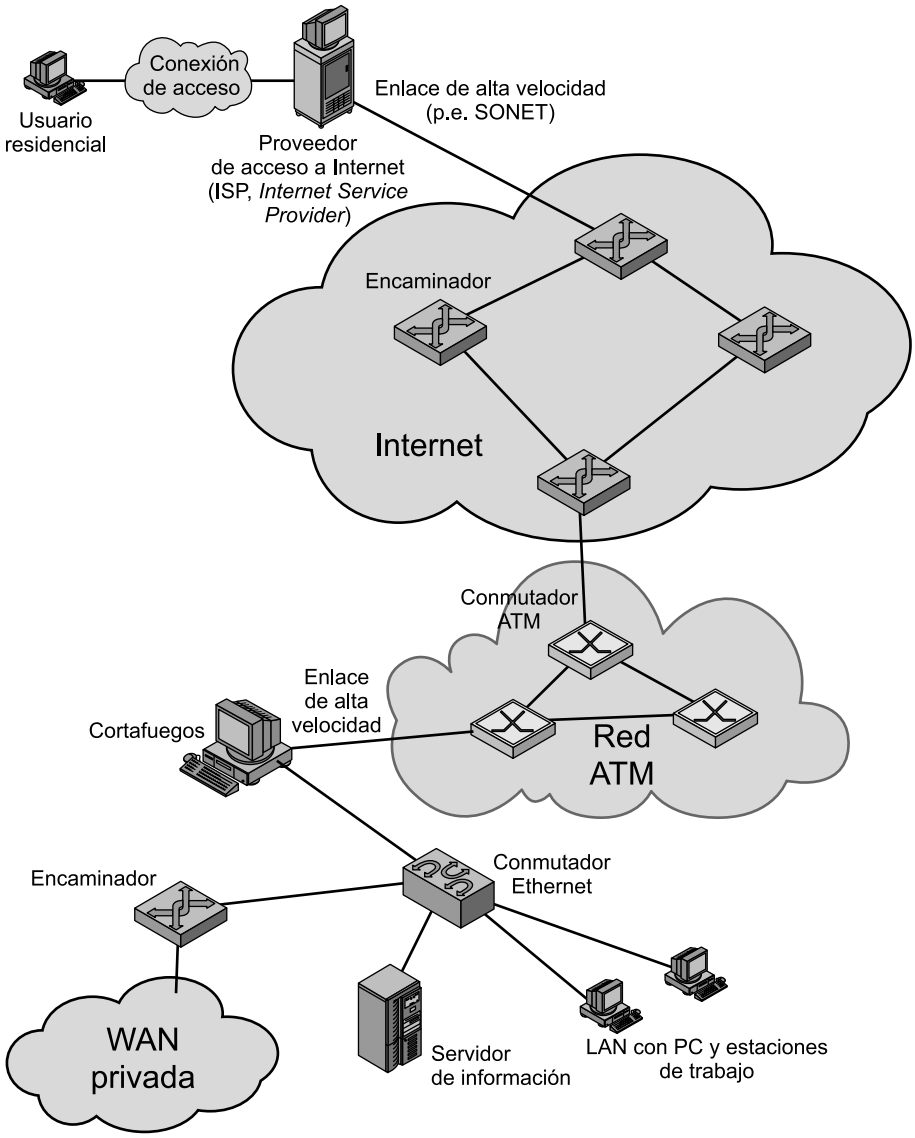


Figura 1.3. Una configuración de red.

módem especial DSL; o un acceso de TV por cable, tecnología que requeriría un cable módem. En cualquier caso, quedan por estudiar, entre otras, cuestiones como la codificación de la señal, el control de errores o la estructura interna de la red de acceso del abonado.

Generalmente, un ISP estará formado por un conjunto de servidores interconectados entre sí (aunque se muestra sólo un servidor) y conectados a Internet a través de un enlace de alta velocidad. Este enlace puede ser, por ejemplo, una línea SONET (*Synchronous Optical NETwork*), estudiada en el Capítulo 8. Internet está formada por una serie de encaminadores interconectados a lo largo de todo el globo terrestre. Los encaminadores transmiten los paquetes de datos desde el origen al destino a través de Internet.

La parte inferior de la Figura 1.3 muestra una LAN implementada con un único conmutador Ethernet. Esta configuración es muy habitual en negocios, oficinas o cualquier tipo de organización de dimensiones reducidas. La LAN se conecta a Internet a través de un equipo cortafuegos (del inglés *firewall*), el cual ofrece servicios de seguridad. También se muestra un encaminador adicional fuera de la LAN conectado a una WAN privada, la cual puede ser una red ATM privada o una red de retransmisión de tramas.

En el diseño de los enlaces que conectan a los distintos elementos mostrados (por ejemplo, entre los encaminadores de Internet, o entre los conmutadores en la red ATM, o entre el abonado y el ISP) quedan pendientes una serie de aspectos como la codificación de la señal y el control de errores. La estructura interna de las distintas redes (de telefonía, Ethernet o ATM) plantea cuestiones adicionales. Todas estas cuestiones, surgidas a partir de la Figura 1.3, serán abordadas en las Partes II, III y IV del presente texto.

CAPÍTULO 2

Arquitectura de protocolos

2.1. ¿Por qué es necesaria una arquitectura de protocolos?

2.2. Una arquitectura de protocolos simple
Un modelo de tres capas
Arquitecturas de protocolos normalizadas

2.3. OSI
El modelo
Normalización dentro del modelo de referencia OSI
Primitivas de servicio y parámetros
Las capas de OSI

2.4. Arquitectura de protocolos TCP/IP
Las capas de TCP/IP
TCP y UDP
Funcionamiento de TCP e IP
Aplicaciones TCP/IP
Interfaces de protocolo

2.5. Lecturas recomendadas y sitios web
Sitio web recomendado

2.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

Apéndice 2A. El protocolo TFTP (*Trivial File Transfer Protocol*)
Introducción al TFTP
Paquetes TFTP
Ejemplo de transferencia
Errores y retardos
Sintaxis, semántica y temporización

CUESTIONES BÁSICAS

- Una arquitectura de protocolos es una estructura en capas de elementos hardware y software que facilita el intercambio de datos entre sistemas y posibilita aplicaciones distribuidas, como el comercio electrónico y la transferencia de archivos.
- En los sistemas de comunicación, en cada una de las capas de la arquitectura de protocolos se implementa uno o más protocolos comunes. Cada protocolo proporciona un conjunto de reglas para el intercambio de datos entre sistemas.
- La arquitectura de protocolos más utilizada es TCP/IP, constituida por las siguientes capas: física, acceso a la red, internet, transporte y aplicación.
- Otra arquitectura de protocolos importante es el modelo de siete capas OSI (*Open Systems Interconnection*).

En este capítulo se establece el contexto para el resto de los conceptos e ideas que se desarrollarán a lo largo del texto. Se muestra cómo los conceptos abordados en las Partes de la II a la V pertenecen a la extensa área de las comunicaciones y redes de computadores. Este capítulo se puede leer en el orden secuencial presentado o puede dejarse para el principio de las Partes III, IV o V[1].

Comenzamos presentando el concepto de arquitectura de protocolos en capas, proponiendo un ejemplo sencillo. A continuación, se define el modelo de referencia para la interconexión de sistemas abiertos OSI (*Open Systems Interconnection*). OSI es una arquitectura normalizada que frecuentemente se utiliza para describir las funciones de un sistema de comunicación, aunque en la actualidad esté implementada escasamente. Posteriormente se estudia la arquitectura de protocolos más importante, la familia de protocolos TCP/IP. TCP/IP es un concepto vinculado a Internet y es el marco de trabajo para el desarrollo de un conjunto completo de normas para las comunicaciones entre computadores. En la actualidad, todos los fabricantes de computadores dan soporte a esta arquitectura.

2.1. ¿POR QUÉ ES NECESARIA UNA ARQUITECTURA DE PROTOCOLOS?

En el intercambio de datos entre computadores, terminales y/u otros dispositivos de procesamiento, los procedimientos involucrados pueden llegar a ser bastante complejos. Considérese, por ejemplo, la transferencia de un archivo entre dos computadores. En este caso, debe haber un camino entre los dos computadores, directo o a través de una red de comunicación, pero además, normalmente se requiere la realización de las siguientes tareas adicionales:

1. El sistema fuente de información debe activar un camino directo de datos o bien debe proporcionar a la red de comunicación la identificación del sistema destino deseado.
2. El sistema fuente debe asegurarse de que el destino está preparado para recibir datos.

[1] Puede ser útil para el lector saltarse este capítulo en una primera lectura para, posteriormente, releerlo con más detenimiento antes de afrontar la lectura de la Parte V.

3. La aplicación de transferencia de archivos en el origen debe asegurarse de que el programa gestor en el destino está preparado para aceptar y almacenar el archivo para el usuario determinado.
4. Si los formatos de los dos archivos son incompatibles en ambos sistemas, uno de los dos deberá realizar una operación de traducción.

Es evidente que debe haber un alto grado de cooperación entre los computadores involucrados. En lugar de implementar toda la lógica para llevar a cabo la comunicación en un único módulo, el problema se divide en subtareas, cada una de las cuales se realiza por separado. En una arquitectura de protocolos, los distintos módulos se disponen formando una pila vertical. Cada capa de la pila realiza el subconjunto de tareas relacionadas entre sí que son necesarias para comunicar con el otro sistema. Por lo general, las funciones más básicas se dejan a la capa inmediatamente inferior, olvidándose en la capa actual de los detalles de estas funciones. Además, cada capa proporciona un conjunto de servicios a la capa inmediatamente superior. Idealmente, las capas deberían estar definidas de forma tal que los cambios en una capa no deberían necesitar cambios en las otras.

Evidentemente, para que haya comunicación se necesitan dos entidades, por lo que debe existir el mismo conjunto de funciones en capas en los dos sistemas. La comunicación se consigue haciendo que las capas correspondientes, o **pares**, intercambien información. Las capas pares se comunican intercambiando bloques de datos que verifican una serie de reglas o convenciones denominadas **protocolo.** Los aspectos clave que definen o caracterizan a un protocolo son:

- **La sintaxis:** establece cuestiones relacionadas con el formato de los bloques de datos.
- **La semántica:** incluye información de control para la coordinación y la gestión de errores.
- **La temporización:** considera aspectos relativos a la sintonización de velocidades y secuenciación.

En el Apéndice 2A se proporciona un ejemplo específico del protocolo normalizado en Internet para la transferencia de archivos TFTP (*Trivial File Transfer Protocol*).

2.2. UNA ARQUITECTURA DE PROTOCOLOS SIMPLE

Habiendo definido el concepto de protocolo, estamos en disposición de definir el concepto de arquitectura de protocolos. A modo de ejemplo, la Figura 2.1 muestra cómo se podría implementar una aplicación de transferencia de archivos. Para ello se usan tres módulos. Las tareas 3 y 4 de la lista anterior se podrían realizar por el módulo de transferencia de archivos. Los dos módulos de ambos sistemas intercambian archivos y órdenes. Sin embargo, en vez de exigir que el módulo de transferencia se encargue de los detalles con los que se realiza el envío de datos y órdenes, dichos módulos delegan en otros módulos que ofrecen el servicio de transmisión. Cada uno de estos se encargará de asegurar que el intercambio de órdenes y datos se realice fiablemente. Entre otras cosas, estos módulos realizarán la tarea 2, por lo que, a partir de este momento, la naturaleza del intercambio entre los sistemas será independiente de la naturaleza de la red que los interconecta. Por tanto, en vez de implementar la interfaz de red en el módulo de servicio de transmisión, tiene sentido prever un módulo adicional de acceso a la red que lleve a cabo la tarea 1, interaccionando con la red.

Resumiendo, el módulo de transferencia de archivos contiene toda la lógica y funcionalidades que son exclusivas de la aplicación, como por ejemplo la transmisión de palabras de paso clave,

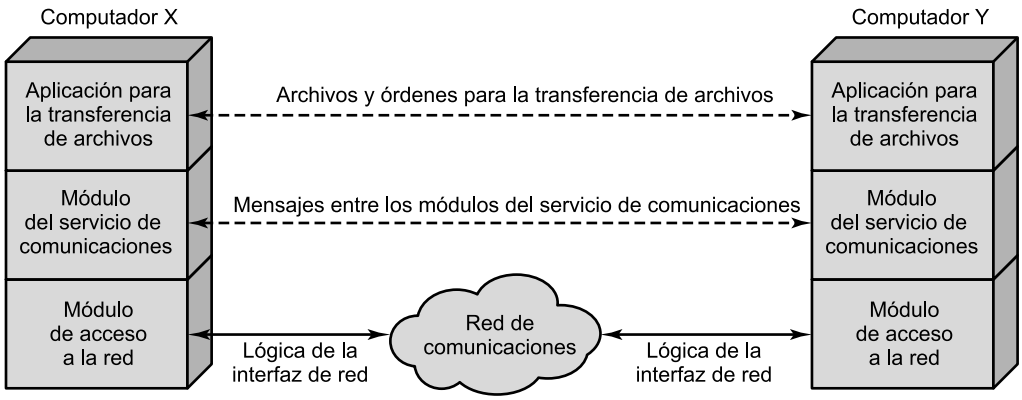

Computador X
Computador Y
Aplicación para la transferencia de archivos
Archivos y órdenes para la transferencia de archivos
Aplicación para la transferencia de archivos
Módulo del servicio de comunicaciones
Mensajes entre los módulos del servicio de comunicaciones
Módulo del servicio de comunicaciones
Módulo de acceso a la red
Lógica de la interfaz de red
Red de comunicaciones
Lógica de la interfaz de red
Módulo de acceso a la red

Figura 2.1. Una arquitectura simplificada para la transferencia de archivos.

de órdenes de archivo o de los registros del archivo. Es necesario que esta información (archivos y órdenes) se transmita de una forma fiable. No obstante, estos mismos requisitos de fiabilidad son compartidos por otro tipo de aplicaciones (como por ejemplo, el correo electrónico y la transferencia de documentos). Por tanto, estas funcionalidades se localizan en el módulo separado del servicio de comunicaciones de tal forma que puedan ser utilizadas por otras aplicaciones. El módulo del servicio de comunicaciones trata de asegurar que los dos computadores estén activos y preparados para la transferencia de datos, así como de seguir la pista de los datos que se intercambian, garantizando su envío. No obstante, estas tareas son independientes del tipo de red que se esté usando. Por tanto, la lógica encargada de tratar con la red se considera en un módulo separado de acceso a la misma. De esta forma, si se modifica la red que se esté usando, sólo se verá afectado el módulo de acceso a la red.

Así, en vez de disponer de un solo módulo que realice todas las tareas involucradas en la comunicación, se considera una estructura consistente en un conjunto de módulos que realizarán todas las funciones. Esta estructura se denomina **arquitectura de protocolos**. Llegados a este punto, la siguiente analogía puede ser esclarecedora. Supóngase que un ejecutivo en una oficina, digamos X, necesita enviar un documento a una oficina Y. El ejecutivo en X prepara el documento y quizá le añada una nota. Esto es análogo a las tareas que realiza la aplicación de transferencia de archivos de la Figura 2.1. A continuación, el ejecutivo le pasa el documento a un secretario o administrativo (A). El A de X mete el documento en un sobre y escribe en él la dirección postal de Y, así como el remite correspondiente a la dirección de X. Puede que en el sobre se escriba igualmente «confidencial». Lo realizado por A corresponde con el módulo del servicio de comunicaciones de la Figura 2.1. Llegados aquí, A pasa el sobre al departamento de envíos. Alguien aquí decide cómo enviar el paquete: mediante correo o mensajería. Se añaden los documentos necesarios al paquete y se realiza el envío. El departamento de envíos corresponde al módulo de acceso a la red de la Figura 2.1. Cuando el paquete llega a Y, se desencadena una serie de operaciones similares en capas. El departamento de envíos en Y recibe el paquete y lo pasa al administrativo correspondiente, dependiendo del destino que figure en el paquete. El A abre el paquete, extrae el documento y se lo pasa al ejecutivo correspondiente.

A continuación, dentro de esta sección se generalizará el ejemplo anterior para presentar una arquitectura de protocolos simplificada. Posteriormente, consideraremos ejemplos más realistas y complejos, como son TCP/IP y OSI.

UN MODELO DE TRES CAPAS

En términos muy generales, se puede afirmar que las comunicaciones involucran a tres agentes: aplicaciones, computadores y redes. Las aplicaciones se ejecutan en computadores que, generalmente, permiten múltiples aplicaciones simultáneas. Los computadores se conectan a redes y los datos a intercambiar se transfieren por la red de un computador a otro. Por tanto, la transferencia de datos desde una aplicación a otra implica, en primer lugar, la obtención de los mismos y, posteriormente, hacerlos llegar a la aplicación destino en el computador remoto.

Teniendo esto presente, parece natural estructurar las tareas de las comunicaciones en tres capas relativamente independientes: la capa de acceso a la red, la capa de transporte y la capa de aplicación.

La **capa de acceso a la red** está relacionada con el intercambio de datos entre el computador y la red a la que está conectado. El computador emisor debe proporcionar a la red la dirección del destino, de tal forma que la red pueda encaminar los datos al destino apropiado. El computador emisor necesitará hacer uso de algunos de los servicios proporcionados por la red, como por ejemplo la gestión de prioridades. Las características del software de esta capa dependerán del tipo de red que se use. Así, se han desarrollado diferentes estándares para conmutación de circuitos, conmutación de paquetes, redes de área local y otros. De esta manera, se pretende separar las funciones que tienen que ver con el acceso a la red en una capa independiente. Haciendo esto, el resto del software de comunicaciones que esté por encima de la capa de acceso a la red no tendrá que ocuparse de las características específicas de la red que se use. El mismo software de las capas superiores debería funcionar correctamente con independencia del tipo de red concreta a la que se esté conectado.

Independientemente de la naturaleza de las aplicaciones que estén intercambiando datos, es un requisito habitual que los datos se intercambien de una manera fiable. Esto es, sería deseable estar seguros de que todos los datos llegan a la aplicación destino y, además, llegan en el mismo orden en que fueron enviados. Como se verá, los mecanismos que proporcionan dicha fiabilidad son independientes de la naturaleza de las aplicaciones. Por tanto, tiene sentido concentrar todos estos procedimientos en una capa común que se comparta por todas las aplicaciones, denominada **capa de transporte**.

Finalmente, la **capa de aplicación** contiene la lógica necesaria para admitir varias aplicaciones de usuario. Para cada tipo distinto de aplicación, como por ejemplo la transferencia de archivos, se necesita un módulo independiente y con características bien diferenciadas.

Las Figuras 2.2 y 2.3 ilustran esta arquitectura sencilla. En la Figura 2.2 se muestran tres computadores conectados a una red. Cada computador contiene software en las capas de acceso a la red, de transporte y de aplicación para una o más aplicaciones. Para una comunicación con éxito, cada entidad deberá tener una dirección única. En realidad, se necesitan dos niveles de direccionamiento. Cada computador en la red debe tener una dirección de red. Esto permite a la red proporcionar los datos al computador apropiado. A su vez, cada aplicación en el computador debe tener una dirección que sea única dentro del propio computador; esto permitirá a la capa de transporte proporcionar los datos a la aplicación apropiada. Estas últimas direcciones son denominadas **puntos de acceso al servicio** (SAP, *Service Access Point*), o también **puertos**, evidenciando que cada aplicación accede individualmente a los servicios proporcionados por la capa de transporte.

La Figura 2.3 muestra cómo se comunican, mediante un protocolo, los módulos en el mismo nivel de computadores diferentes. Veamos su funcionamiento. Supóngase que una aplicación, asociada al SAP 1 en el computador X, quiere transmitir un mensaje a otra aplicación, asociada al

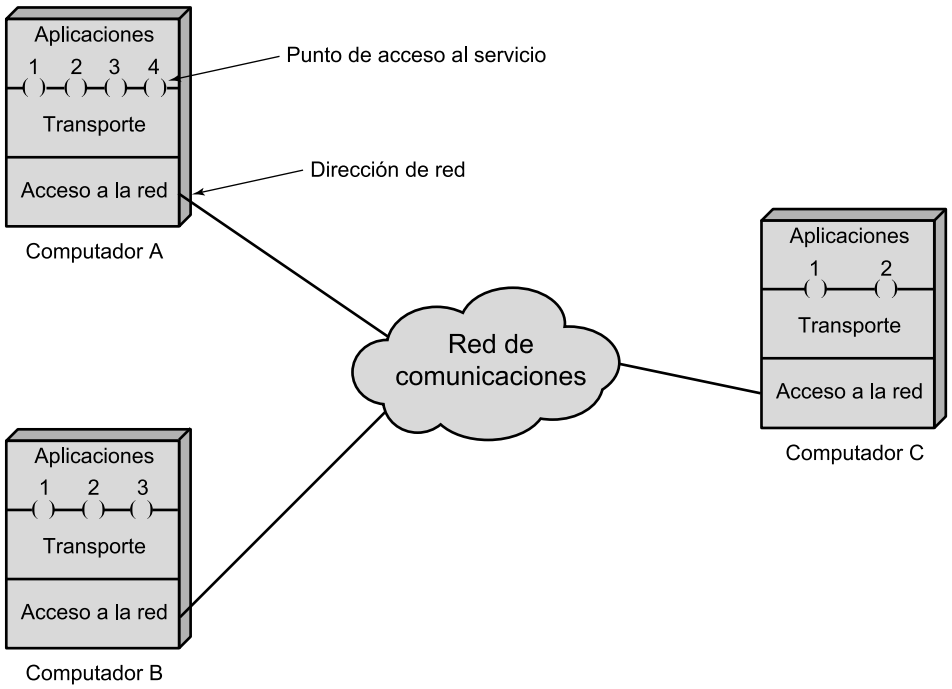


Figura 2.2. Redes y arquitecturas de protocolos.

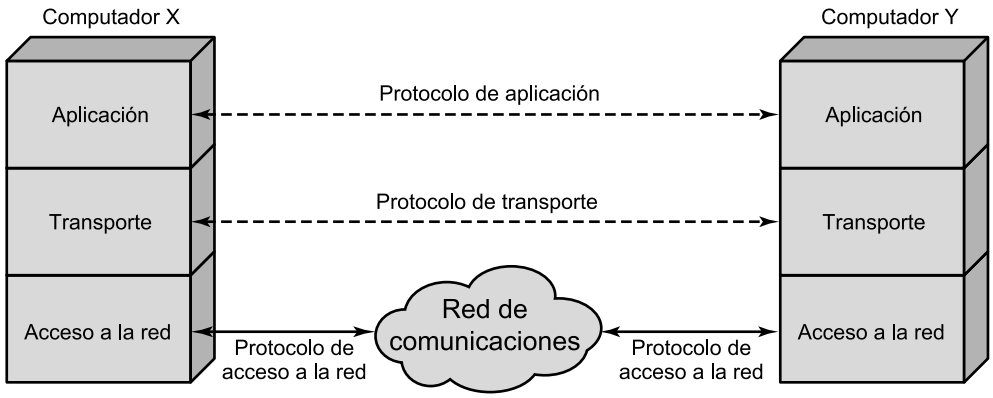


Figura 2.3. Protocolos en una arquitectura simplificada.

SAP 2 del computador Y. La aplicación en X pasa el mensaje a la capa de transporte con instrucciones para que lo envíe al SAP 2 de Y. A su vez, la capa de transporte pasa el mensaje a la capa de acceso a la red, la cual proporciona las instrucciones necesarias a la red para que envíe el mensaje a Y. Debe observarse que la red no necesita conocer la dirección del punto de acceso al servicio en el destino. Todo lo que necesita conocer es que los datos están dirigidos al computador Y.

Para controlar esta operación, se debe transmitir información de control junto a los datos del usuario, como así se muestra en la Figura 2.4. Supongamos que la aplicación emisora genera un bloque de datos y se lo pasa a la capa de transporte. Esta última puede fraccionar el bloque en unidades más pequeñas para hacerlas más manejables. A cada una de estas pequeñas unidades, la

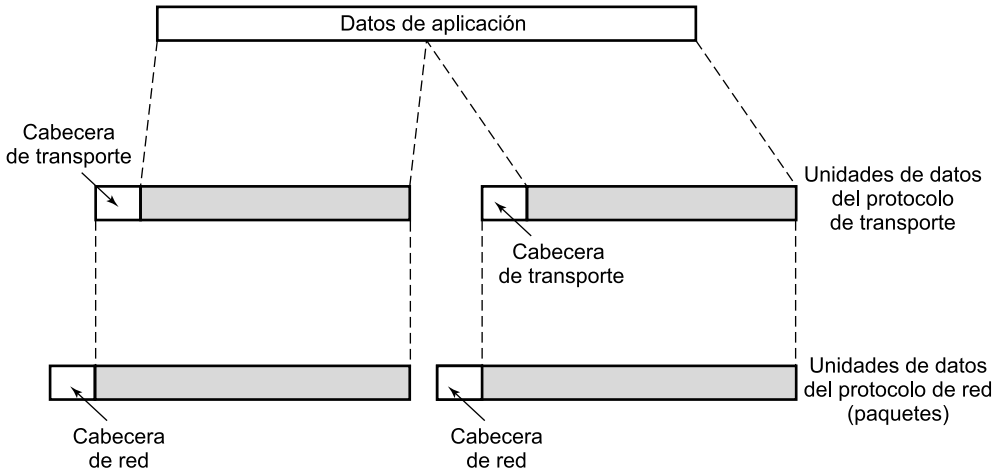


Figura 2.4. Unidades de datos de los protocolos.

capa de transporte le añadirá una cabecera, que contendrá información de control de acuerdo con el protocolo. La unión de los datos generados por la capa superior, junto con la información de control de la capa actual, se denomina **unidad de datos del protocolo** (PDU, *Protocol Data Unit*). En este caso, se denominará como **PDU de transporte**. La cabecera en cada PDU de transporte contiene información de control que será usada por el protocolo de transporte par en el computador Y. La información que se debe incluir en la cabecera puede ser por ejemplo:

- **SAP destino:** cuando la capa de transporte destino reciba la PDU de transporte, deberá saber a quién van destinados los datos.
- **Número de secuencia:** ya que el protocolo de transporte está enviando una secuencia de PDU, éstas se numerarán secuencialmente para que, si llegan desordenadas, la entidad de transporte destino sea capaz de ordenarlas.
- **Código de detección de error:** la entidad de transporte emisora debe incluir un código obtenido en función del resto de la PDU. El protocolo de transporte receptor realiza el mismo cálculo y compara los resultados con el código recibido. Si hay discrepancia se concluirá que ha habido un error en la transmisión y, en ese caso, el receptor podrá descartar la PDU y adoptar las acciones oportunas para su corrección.

El siguiente paso en la capa de transporte es pasar cada una de las PDU a la capa de red, con la instrucción de que sea transmitida al computador destino. Para satisfacer este requerimiento, el protocolo de acceso a la red debe pasar los datos a la red con una solicitud de transmisión. Como anteriormente, esta operación requiere el uso de información de control. En este caso, el protocolo de acceso a la red añade la cabecera de acceso a la red a los datos provenientes de la capa de transporte, creando así la PDU de acceso a la red. A modo de ejemplo, la cabecera debe contener la siguiente información:

- **La dirección del computador destino**: la red debe conocer a quién (qué computador de la red) debe entregar los datos.
- **Solicitud de recursos**: el protocolo de acceso a la red puede pedir a la red que realice algunas funciones, como por ejemplo, gestionar prioridades.

En la Figura 2.5 se conjugan todos estos conceptos, mostrando la interacción desarrollada entre los módulos para transferir un bloque de datos. Supongamos que el módulo de transferencia de

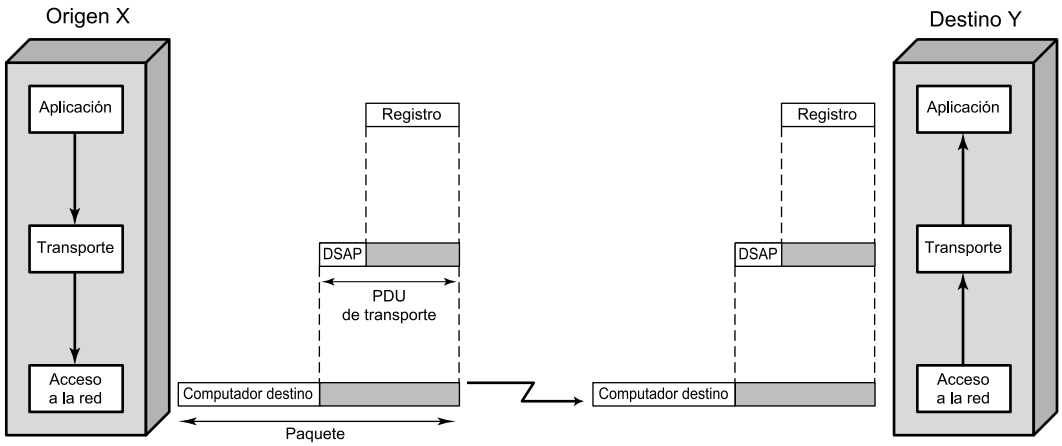


Figura 2.5. Funcionamiento de una arquitectura de protocolos.

archivos en el computador X está transfiriendo, registro a registro, un archivo al computador Y. Cada registro se pasa al módulo de la capa de transporte. Se puede describir esta acción como si se tratase de una orden o una llamada a un procedimiento. Los posibles argumentos pasados en la llamada a este procedimiento serán la dirección del destino, el SAP destino y el registro del archivo. La capa de transporte añade el punto de acceso al servicio e información de control adicional, que se agregará al registro para formar la PDU de transporte. Ésta se pasa a la capa inferior de acceso a la red mediante la llamada a otro procedimiento. En este caso, los argumentos para esta llamada serán la dirección del computador destino y la unidad de datos del protocolo de transporte. La capa de acceso a la red usará esta información para construir la PDU de red. La PDU de transporte es el campo de datos de la PDU de red, y su cabecera contendrá información relativa a las direcciones origen y destino. Nótese que la cabecera de transporte no es «visible» al nivel de acceso a la red; en otras palabras, a dicho nivel no le concierne el contenido concreto de la PDU de transporte.

La red acepta la PDU de transporte de X y la transmite a Y. El módulo de acceso a la red en Y recibe la PDU, elimina la cabecera y pasa la PDU de transporte adjunta al módulo de la capa de transporte de Y. La capa de transporte examina la cabecera de la unidad de datos del protocolo de transporte y, en función del contenido del campo de la cabecera que contenga el SAP, entregará el registro correspondiente a la aplicación pertinente, en este caso, al módulo de transferencia de archivos de Y.

ARQUITECTURAS DE PROTOCOLOS NORMALIZADAS

Cuando se desea establecer una comunicación entre computadores de diferentes fabricantes, el desarrollo del software puede convertirse en una pesadilla. Los distintos fabricantes pueden hacer uso de distintos formatos y protocolos de intercambio de datos. Incluso dentro de una misma línea de productos de un fabricante dado, los diferentes modelos pueden comunicarse de forma diferente.

Con la proliferación tanto de las comunicaciones entre computadores como de las redes, el desarrollo de software de comunicaciones de propósito específico es demasiado costoso para ser aceptable. La única alternativa para los fabricantes es adoptar e implementar un conjunto de convenciones comunes. Para que esto ocurra, es necesaria la normalización. Los estándares tienen las siguientes ventajas:

- Los fabricantes están motivados para implementar las normalizaciones con la esperanza de que, debido al uso generalizado de las normas, sus productos tendrán un mercado mayor.
- Los clientes pueden exigir que cualquier fabricante implemente los estándares.

Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de comunicación: el conjunto de protocolos TCP/IP y el modelo de referencia de OSI. TCP/IP es, con diferencia, la arquitectura más usada. OSI, aun siendo bien conocida, nunca ha llegado a alcanzar las promesas iniciales. Además de las anteriores, hay otra arquitectura propietaria ampliamente utilizada: la SNA (*System Network Architecture*) de IBM. En lo que resta de este capítulo se estudiará OSI y TCP/IP.

2.3. OSI

Los estándares son necesarios para promover la interoperatividad entre los equipos de distintos fabricantes, así como para facilitar economías de gran escala. Debido a la complejidad que implican las comunicaciones, un solo estándar no es suficiente. En su lugar, las distintas funcionalidades deberían dividirse en partes más manejables, estructurándose en una arquitectura de comunicaciones. La arquitectura constituirá, por tanto, el marco de trabajo para el proceso de normalización. Esta línea argumental condujo a la Organización Internacional de Estandarización (ISO, *Internacional Organization for Standarization*) en 1977 a establecer un subcomité para el desarrollo de tal arquitectura. El resultado fue el modelo de referencia OSI. Aunque los elementos esenciales del modelo se definieron rápidamente, la norma ISO final, ISO 7498, no fue publicada hasta 1984. La CCITT (en la actualidad denominada UIT-T) definió igualmente una versión técnicamente compatible con la anterior, denominada X.200.

EL MODELO

Una técnica muy aceptada para estructurar los problemas, y así fue adoptada por ISO, es la división en capas. En esta técnica, las funciones de comunicación se distribuyen en un conjunto jerárquico de capas. Cada capa realiza un subconjunto de tareas, relacionadas entre sí, de entre las necesarias para llegar a comunicarse con otros sistemas. Por otra parte, cada capa se sustenta en la capa inmediatamente inferior, la cual realizará funciones más primitivas, ocultando los detalles a las capas superiores. Una capa proporciona servicios a la capa inmediatamente superior. Idealmente, las capas deberían estar definidas para que los cambios en una capa no implicaran cambios en las otras capas. De esta forma, el problema se descompone en varios subproblemas más abordables.

La labor de ISO consistió en definir el conjunto de capas, así como los servicios a realizar por cada una de ellas. La división debería agrupar a las funciones que fueran conceptualmente próximas en un número suficiente, tal que cada capa fuese lo suficientemente pequeña, pero sin llegar a definir demasiadas para evitar así sobrecargas en el procesamiento. Las directrices generales que se adoptaron en el diseño se resumen en la Tabla 2.1. El modelo de referencia resultante tiene siete capas, las cuales son mostradas, junto a una breve definición, en la Figura 2.6. La Tabla 2.2 proporciona la justificación para la selección de las capas argumentada por ISO.

La Figura 2.7 muestra la arquitectura OSI. Cada sistema debe contener las siete capas. La comunicación se realiza entre las dos aplicaciones de los dos computadores, etiquetadas como aplicación X e Y en la figura. Si la aplicación X quiere transmitir un mensaje a la aplicación Y, invoca

Tabla 2.1. Directrices seguidas en la definición de las capas OSI (X.200).

1.	No crear demasiadas capas de tal forma que la descripción e integración de las capas implique más dificultades de las necesarias.
2.	Crear una separación entre capas en todo punto en el que la descripción del servicio sea reducida y el número de interacciones a través de dicha separación sea pequeña.
3.	Crear capas separadas allá donde las funciones sean manifiestamente diferentes tanto en la tarea a realizar como en la tecnología involucrada.
4.	Agrupar funciones similares en la misma capa.
5.	Fijar las separaciones en aquellos puntos en los que la experiencia acumulada haya demostrado su utilidad.
6.	Crear capas que puedan ser rediseñadas en su totalidad y los protocolos cambiados de forma drástica para aprovechar eficazmente cualquier innovación que surja tanto en la arquitectura, el hardware o tecnologías software, sin tener que modificar los servicios ofrecidos o usados por las capas adyacentes.
7.	Crear una separación allá donde sea conveniente tener la correspondiente interfaz normalizada.
8.	Crear una capa donde haya necesidad de un nivel distinto de abstracción (morfológico, sintáctico o semántico) a la hora de gestionar los datos.
9.	Permitir que los cambios en las funciones o protocolos se puedan realizar sin afectar a otras capas.
10.	Para cada capa establecer separaciones sólo con sus capas inmediatamente superiores o inferiores.
	Las siguientes premisas se propusieron igualmente para definir subcapas:
11.	Crear posteriores subagrupamientos y reestructurar las funciones formando subcapas dentro de una capa en aquellos casos en los que se necesiten diferentes servicios de comunicación.
12.	Crear, allá donde sea necesario, dos o más subcapas con una funcionalidad común, y mínima, para permitir operar con las capas adyacentes.
13.	Permitir la no utilización de una subcapa dada.

a la capa de aplicación (capa 7). La capa 7 establece una relación paritaria con la capa 7 del computador destino, usando el protocolo de la capa 7 (protocolo de aplicación). Este protocolo necesita los servicios de la capa 6, de forma tal que las dos entidades de la capa 6 usan un protocolo común y conocido, y así sucesivamente hasta llegar a la capa física, en la que realmente se transmiten los bits a través del medio físico.

Nótese que, exceptuando la capa física, no hay comunicación directa entre las capas pares. Esto es, por encima de la capa física, cada entidad de protocolo pasa los datos hacia la capa inferior contigua, para que ésta los envíe a su entidad par. Es más, el modelo OSI no requiere que los dos sistemas estén conectados directamente, ni siquiera en la capa física. Por ejemplo, para proporcionar el enlace de comunicación se puede utilizar una red de conmutación de paquetes o de conmutación de circuitos.

La Figura 2.7 también muestra cómo se usan las unidades de datos de protocolo (PDU) en la arquitectura OSI. En primer lugar, considérese la forma más habitual de implementar un protocolo.

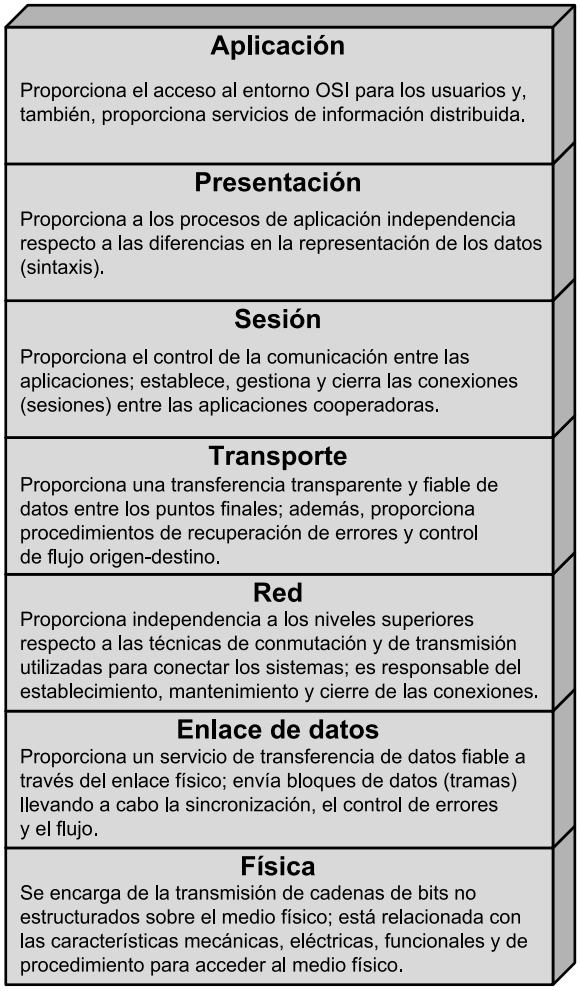

Aplicación
Proporciona el acceso al entorno OSI para los usuarios y, también, proporciona servicios de información distribuida.
Presentación
Proporciona a los procesos de aplicación independencia respecto a las diferencias en la representación de los datos (sintaxis).
Sesión
Proporciona el control de la comunicación entre las aplicaciones; establece, gestiona y cierra las conexiones (sesiones) entre las aplicaciones cooperadoras.
Transporte
Proporciona una transferencia transparente y fiable de datos entre los puntos finales; además, proporciona procedimientos de recuperación de errores y control de flujo origen-destino.
Red
Proporciona independencia a los niveles superiores respecto a las técnicas de conmutación y de transmisión utilizadas para conectar los sistemas; es responsable del establecimiento, mantenimiento y cierre de las conexiones.
Enlace de datos
Proporciona un servicio de transferencia de datos fiable a través del enlace físico; envía bloques de datos (tramas) llevando a cabo la sincronización, el control de errores y el flujo.
Física
Se encarga de la transmisión de cadenas de bits no estructurados sobre el medio físico; está relacionada con las características mecánicas, eléctricas, funcionales y de procedimiento para acceder al medio físico.

Figura 2.6. Las capas de OSI.

Cuando la aplicación X tiene un mensaje para enviar a la aplicación Y, transfiere estos datos a una entidad de la capa de aplicación. A los datos se les añade una cabecera que contiene información necesaria para el protocolo de la capa 7 (encapsulado). Seguidamente, los datos originales más la cabecera se pasan como una unidad a la capa 6. La entidad de presentación trata la unidad completa como si de datos se tratara y le añade su propia cabecera (un segundo encapsulado). Este proceso continúa hacia abajo hasta llegar a la capa 2, que normalmente añade una cabecera y una cola. La unidad de datos de la capa 2, llamada trama, se pasa al medio de transmisión mediante la capa física. En el destino, al recibir la trama, ocurre el proceso inverso. Conforme los datos ascienden, cada capa elimina la cabecera más externa, actúa sobre la información de protocolo contenida en ella y pasa el resto de la información hacia la capa inmediatamente superior.

En cada etapa del proceso, cada una de las capas puede fragmentar la unidad de datos que recibe de la capa inmediatamente superior en varias partes, de acuerdo con sus propias necesidades. Estas unidades de datos deben ser ensambladas por la capa par correspondiente antes de pasarlas a la capa superior.

Tabla 2.2. Justificación de las capas OSI (X.200)

1. Es esencial que la arquitectura permita la utilización de una variedad realista de medios físicos para la interconexión con diferentes procedimientos de control (por ejemplo, V.24, V.25, etc.). La aplicación de los principios 3, 5 y 8 (Tabla 2.1) nos conduce a la identificación de la **capa física** como la capa más baja en la arquitectura.
2. Algunos medios de comunicación físicos (por ejemplo, las líneas telefónicas) requieren técnicas específicas para usarlos, al transmitir datos entre sistemas a pesar de sufrir una tasa de error elevada (una tasa de error no aceptable para la gran mayoría de las aplicaciones). Estas técnicas específicas se utilizan en procedimientos de control del enlace de datos que han sido estudiados y normalizados durante una serie de años. También se debe reconocer que los nuevos medios de comunicación física (por ejemplo, la fibra óptica) requerirán diferentes procedimientos de control del enlace de datos. La aplicación de los principios 3, 5 y 8 nos conduce a la identificación de la **capa del enlace de datos** situada encima de la capa física en la arquitectura.
3. En la arquitectura de sistemas abiertos, algunos sistemas abiertos actuarán como el destino final de los datos. Algunos sistemas abiertos podrían actuar solamente como nodos intermedios (reenviando los datos a otros sistemas). La aplicación de los principios 3, 5 y 7 nos conduce a la identificación de la **capa de red** encima de la capa del enlace de datos. Los protocolos dependientes de la red, como por ejemplo el encaminamiento, se agrupan en esta capa. Así, la capa de red proporcionará un camino de conexión (conexión de red) entre un par de entidades de transporte incluyendo el caso en el que estén involucrados nodos intermedios.
4. El control del transporte de los datos desde el sistema final origen al sistema final destino (que no se lleva a cabo en nodos intermedios) es la última función necesaria para proporcionar la totalidad del servicio de transporte. Así, la capa superior situada justo encima de la capa de red es la **capa de transporte**. Esta capa libera a las entidades de capas superiores de cualquier preocupación sobre el transporte de datos entre ellas.
5. Existe una necesidad de organizar y sincronizar el diálogo y controlar el intercambio de datos. La aplicación de los principios 3 y 4 nos conduce a la identificación de la **capa de sesión** encima de la capa de transporte.
6. El conjunto restante de funciones de interés general son aquellas relacionadas con la representación y la manipulación de datos estructurados, para el beneficio de los programas de aplicación. La aplicación de los principios 3 y 4 nos conduce a la identificación de la **capa de presentación** encima de la capa de sesión.
7. Finalmente, existen aplicaciones consistentes en procesos de aplicación que procesan la información. Un aspecto de estos procesos de aplicación y los protocolos mediante los que se comunican comprenden la **capa de aplicación**, que es la capa más alta de la arquitectura.

NORMALIZACIÓN DENTRO DEL MODELO DE REFERENCIA OSI[2]

La principal motivación para el desarrollo del modelo OSI fue proporcionar un modelo de referencia para la normalización. Dentro del modelo, en cada capa se pueden desarrollar uno o más protocolos. El modelo define en términos generales las funciones que se deben realizar en cada capa y simplifica el procedimiento de la normalización ya que:

- Como las funciones de cada capa están bien definidas, para cada una de ellas, el establecimiento de normas o estándares se puede desarrollar independiente y simultáneamente. Esto acelera el proceso de normalización.

[2] Los conceptos que aquí se introducen son igualmente válidos para la arquitectura TCP/IP.

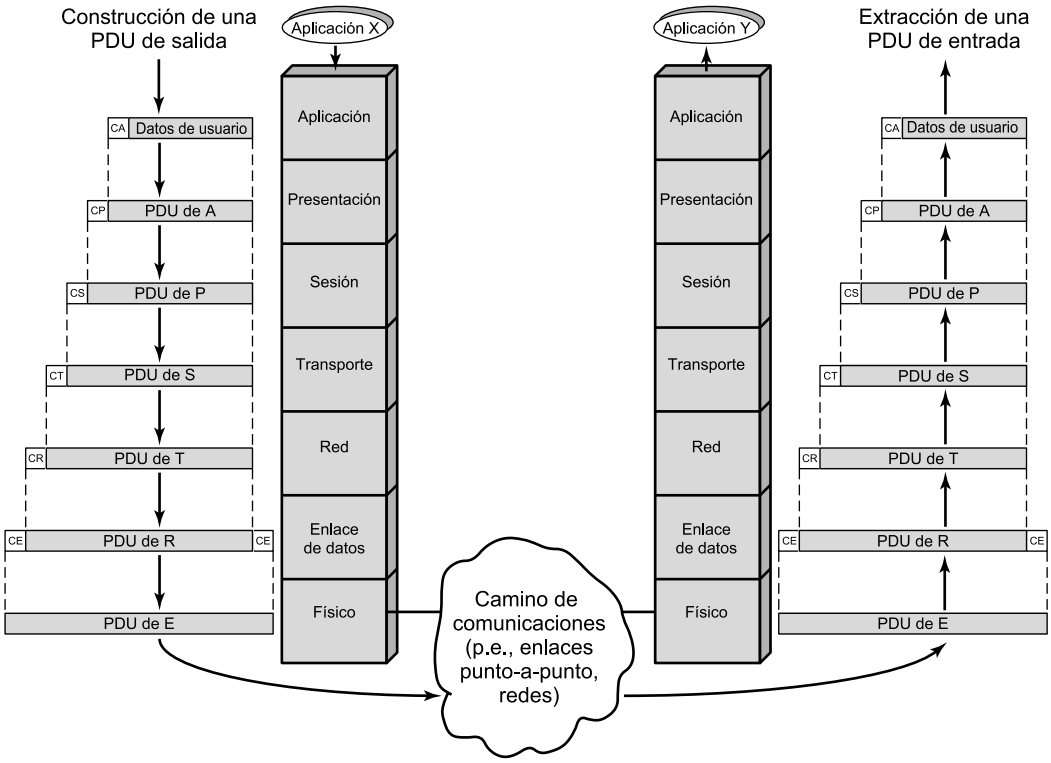


Figura 2.7. El entorno OSI.

- Como los límites entre capas están bien definidos, los cambios que se realicen en los estándares para una capa dada no afectan al software de las otras. Esto hace que sea más fácil introducir nuevas normalizaciones.

La Figura 2.8 muestra el uso del modelo de referencia OSI. La función global de comunicación se descompone en 7 capas distintas, utilizando los principios indicados en la Tabla 2.1. Estos principios esencialmente vienen a ser los mismos que rigen en el diseño modular. Esto es, la función global se descompone en una serie de módulos, haciendo que las interfaces entre módulos sean tan simples como sea posible. Además, se utiliza el principio de ocultación de la información: las capas inferiores abordan ciertos detalles de tal manera que las capas superiores sean ajenas a las particularidades de estos detalles. Dentro de cada capa, se suministra el servicio proporcionado a la capa inmediatamente superior, a la vez que se implementa el protocolo con la capa par en el sistema remoto.

La Figura 2.9 muestra de una forma más específica la naturaleza de la normalización requerida en cada capa. Existen tres elementos clave:

- **Especificación del protocolo:** dos entidades en la misma capa en sistemas diferentes cooperan e interactúan por medio del protocolo. El protocolo se debe especificar con precisión, ya que están implicados dos sistemas abiertos diferentes. Esto incluye el formato de la unidad de datos del protocolo, la semántica de todos los campos, así como la secuencia permitida de PDU.

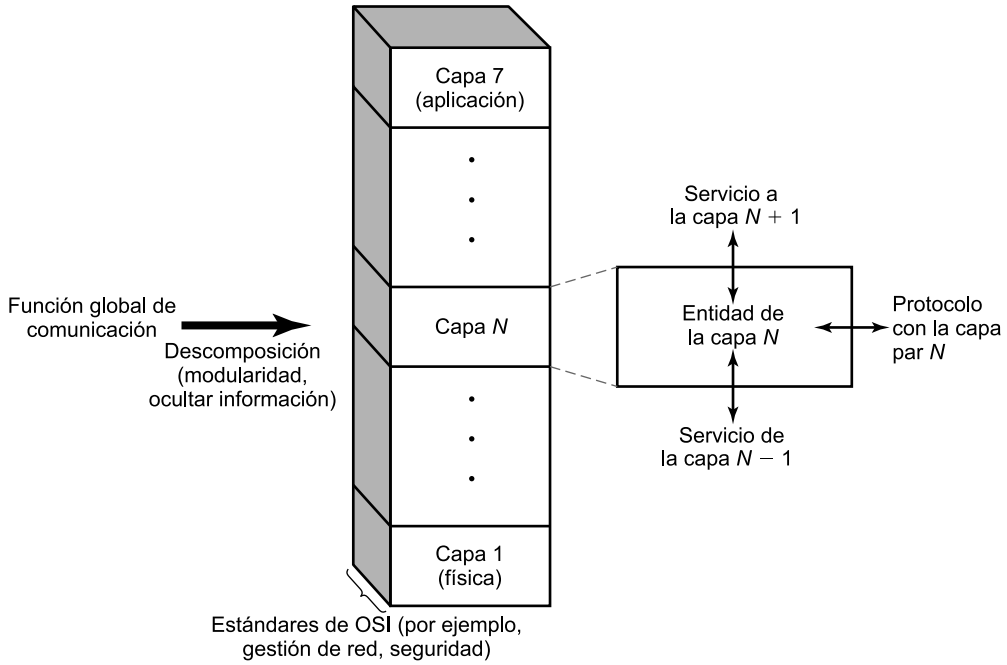


Figura 2.8. La arquitectura OSI como un modelo de referencia para las normalizaciones.

- **Definición del servicio:** además del protocolo o protocolos que operan en una capa dada, se necesitan normalizaciones para los servicios que cada capa ofrece a la capa inmediatamente superior. Normalmente, la definición de los servicios es equivalente a una descripción funcional que definiera los servicios proporcionados, pero sin especificar cómo se están proporcionando.
- **Direccionamiento:** cada capa suministra servicios a las entidades de la capa inmediatamente superior. Las entidades se identifican mediante un punto de acceso al servicio (SAP). Así, un punto de acceso al servicio de red (NSAP, *Network SAP*) identifica a una entidad de transporte usuaria del servicio de red.

En los sistemas abiertos, la necesidad de proporcionar una especificación precisa del protocolo se evidencia por sí sola. Los otros dos elementos de la lista anterior requieren más comentarios. Con respecto a la definición de servicios, la motivación para proporcionar sólo una definición funcional es la siguiente. Primero, la interacción entre capas adyacentes tiene lugar dentro de los confines de un único sistema abierto y, por tanto, le incumbe sólo a él. Así, mientras las capas pares en diferentes sistemas proporcionen los mismos servicios a las capas inmediatamente superiores, los detalles de cómo se suministran los servicios pueden diferir de un sistema a otro sin que ello implique pérdida de interoperatividad. Segundo, es frecuente que las capas adyacentes estén implementadas en el mismo procesador. En estas circunstancias, sería interesante dejar libre al programador del sistema para que utilice el hardware y el sistema operativo para que proporcionen una interfaz que sea lo más eficiente posible.

En lo que se refiere al direccionamiento, la utilización de un mecanismo de direccionamiento en cada capa, materializado en el SAP, permite que cada capa multiplexe varios usuarios de la capa inmediatamente superior. La multiplexación puede que no se lleve a cabo en todos los niveles. No obstante, el modelo lo permite.

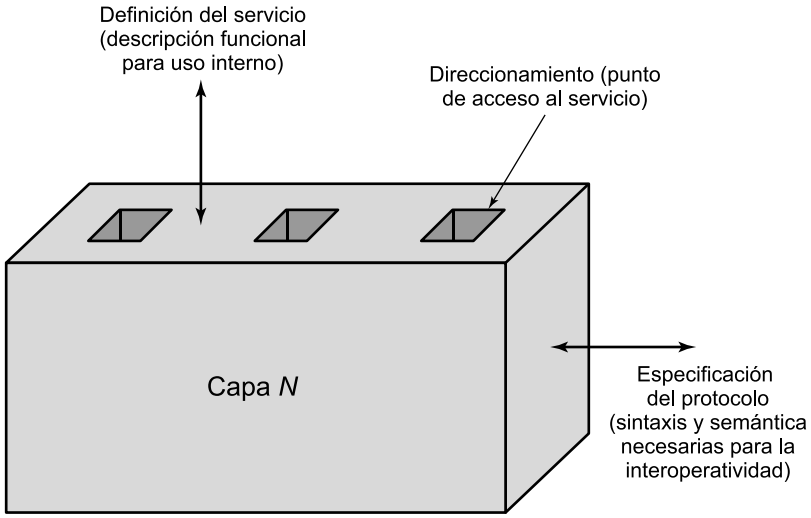


Figura 2.9. Elementos a normalizar en cada capa.

PARÁMETROS Y PRIMITIVAS DE SERVICIO

En la arquitectura OSI los servicios entre capas adyacentes se describen en términos de primitivas y mediante los parámetros involucrados. Una primitiva especifica la función que se va a llevar a cabo y los parámetros se utilizan para pasar datos e información de control. La forma concreta que adopte la primitiva dependerá de la implementación. Un ejemplo es una llamada a un procedimiento.

Para definir las interacciones entre las capas adyacentes de la arquitectura se utilizan cuatro tipos de primitivas (X.210). Éstas se definen en la Tabla 2.3. En la Figura 2.10a se muestra la ordenación temporal de estos eventos. A modo de ejemplo, considere la transferencia de datos desde una entidad (*N*) a su entidad par (*N*) en otro sistema. En esta situación se verifican los siguientes hechos:

1. La entidad origen (*N*) invoca a su entidad ($N - 1$) con una primitiva de *solicitud*. Asociados a esta primitiva están los parámetros necesarios, como por ejemplo, los datos que se van a transmitir y la dirección destino.

Tabla 2.3. Tipos de primitivas de servicio.

SOLICITUD	Primitiva emitida por el usuario del servicio para invocar algún servicio y pasar los parámetros necesarios para especificar completamente el servicio solicitado.
INDICACIÓN	Primitiva emitida por el proveedor del servicio para: **1.** indicar que ha sido invocado un procedimiento por el usuario de servicio par en la conexión y para suministrar los parámetros asociados, o **2.** notificar al usuario del servicio una acción iniciada por el suministrador.
RESPUESTA	Primitiva emitida por el usuario del servicio para confirmar o completar algún procedimiento invocado previamente mediante una indicación a ese usuario.
CONFIRMACIÓN	Primitiva emitida por el proveedor del servicio para confirmar o completar algún procedimiento invocado previamente mediante una solicitud por parte del usuario del servicio.

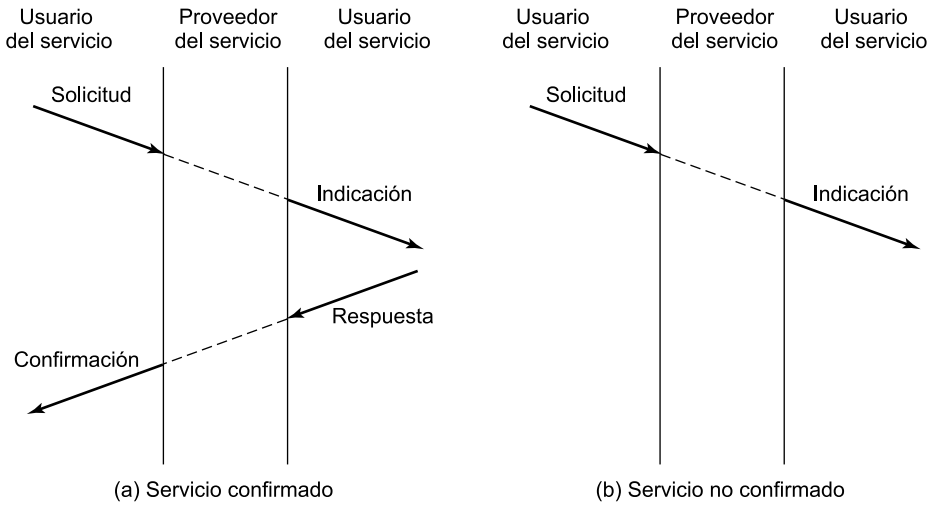


Figura 2.10. Diagramas temporales de las primitivas de servicio.

2. La entidad origen ($N-1$) prepara una PDU ($N-1$) para enviársela a su entidad par ($N-1$).
3. La entidad destino ($N-1$) entrega los datos al destino apropiado (N) a través de la primitiva de *indicación*, que incluye como parámetros los datos y la dirección origen.
4. Si se requiere una confirmación, la entidad destino (N) emite una primitiva de *respuesta* a su entidad (N-1).
5. La entidad ($N-1$) convierte la confirmación en una PDU ($N-1$).
6. La confirmación se entrega a la entidad (N) a través de una primitiva de *confirmación*.

Esta secuencia de eventos se conoce como un **servicio confirmado**, ya que el que inicia la transferencia recibe una confirmación de que el servicio solicitado ha tenido el efecto deseado en el otro extremo. Si solamente se invocan las primitivas de solicitud e indicación (correspondientes a los pasos 1 a 3), entonces se denomina **servicio no confirmado**: la entidad que inicia la transferencia no recibe confirmación de que la acción solicitada haya tenido lugar (Figura 2.10b).

LAS CAPAS DE OSI

En esta sección se estudian brevemente cada una de la capas y, donde sea pertinente, se proporcionan ejemplos de normalizaciones para los protocolos de estas capas.

Capa física

La capa física se encarga de la interfaz física entre los dispositivos. Además, define las reglas que rigen en la transmisión de los bits. La capa física tiene cuatro características importantes:

- **Mecánicas:** relacionadas con las propiedades físicas de la interfaz con el medio de transmisión. Normalmente, dentro de estas características se incluye la especificación del conector que transmite las señales a través de conductores. A estos últimos se les denominan circuitos.
- **Eléctricas:** especifican cómo se representan los bits (por ejemplo, en términos de niveles de tensión), así como su velocidad de transmisión.

- **Funcionales:** especifican las funciones que realiza cada uno de los circuitos de la interfaz física entre el sistema y el medio de transmisión.
- **De procedimiento:** especifican la secuencia de eventos que se llevan a cabo en el intercambio del flujo de bits a través del medio físico.

En el Capítulo 6 se estudian con detalle los protocolos de la capa física. Algunos ejemplos de estándares de esta capa son el EIA-232-F y algunas secciones de los estándares de comunicaciones inalámbricas y LAN.

Capa de enlace de datos

Mientras que la capa física proporciona exclusivamente un servicio de transmisión de datos, la capa de enlace de datos intenta hacer que el enlace físico sea fiable. Además proporciona los medios para activar, mantener y desactivar el enlace. El principal servicio proporcionado por la capa de enlace de datos a las capas superiores es el de detección y control de errores. Así, si se dispone de un protocolo en la capa de enlace de datos completamente operativo, la capa adyacente superior puede suponer que la transmisión está libre de errores. Sin embargo, si la comunicación se realiza entre dos sistemas que no estén directamente conectados, la conexión constará de varios enlaces de datos en serie, cada uno operando independientemente. Por tanto, en este último caso, la capa superior no estará libre de la responsabilidad del control de errores.

El Capítulo 7 se dedica a los protocolos de enlace de datos. Algunos ejemplos de estándares en esta capa son HDLC y LLC.

Capa de red

La capa de red realiza la transferencia de información entre sistemas finales a través de algún tipo de red de comunicación. Libera a las capas superiores de la necesidad de tener conocimiento sobre la transmisión de datos subyacente y las tecnologías de conmutación utilizadas para conectar los sistemas. En esta capa, el computador establecerá un diálogo con la red para especificar la dirección destino y solicitar ciertos servicios, como por ejemplo, la gestión de prioridades.

Existe un amplio abanico de posibilidades para que los servicios de comunicación intermedios sean gestionados por la capa de red. En el extremo más sencillo están los enlaces punto-a-punto directos entre estaciones. En este caso no se necesita capa de red, ya que la capa de enlace de datos puede proporcionar las funciones de gestión del enlace necesarias.

Siguiendo en orden de complejidad creciente, podemos considerar un sistema conectado a través de una única red, como una red de conmutación de circuitos o de conmutación de paquetes. Un ejemplo de esta situación es el nivel de paquetes del estándar X.25. La Figura 2.11 muestra cómo la presencia de una red se encuadra dentro de la arquitectura OSI. Las tres capas inferiores están relacionadas con la conexión y la comunicación con la red. Los paquetes creados por el sistema final pasan a través de uno o más nodos de la red, que actúan como retransmisores entre los dos sistemas finales. Los nodos de la red implementan las capas 1 a 3 de la arquitectura. En la figura anterior se muestran dos sistemas finales conectados a través de un único nodo de red. La capa 3 en el nodo realiza las funciones de conmutación y encaminamiento. Dentro del nodo, existen dos capas del enlace de datos y dos capas físicas, correspondientes a los enlaces con los dos

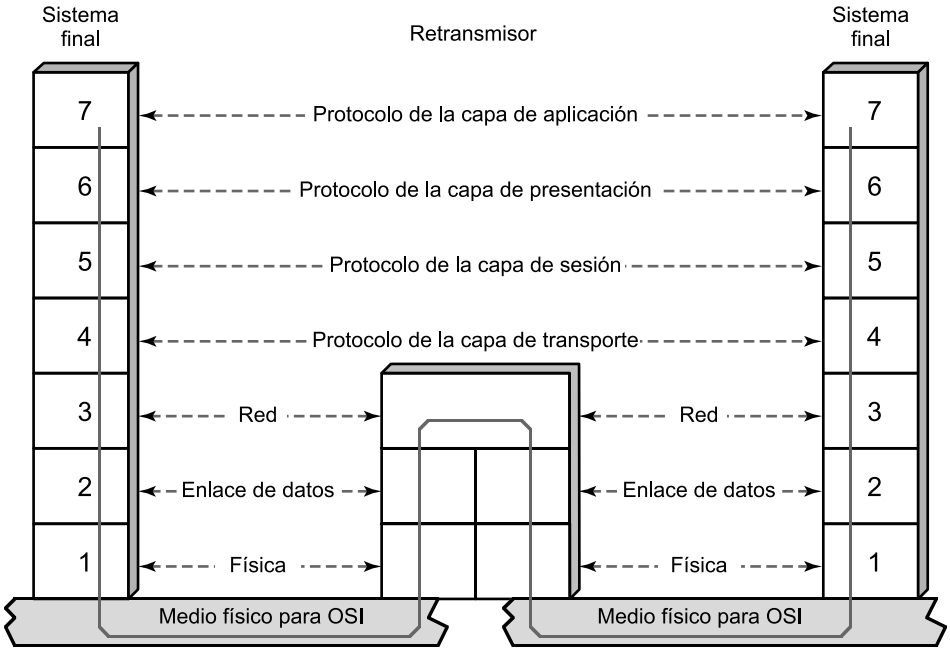


Figura 2.11. Utilización de un retransmisor.

sistemas finales. Cada capa del enlace de datos (y física) opera independientemente para proporcionar el servicio a la capa de red sobre su respectivo enlace. Las cuatro capas superiores son protocolos «extremo-a-extremo» entre los sistemas finales.

En el otro extremo de complejidad, una configuración para la capa de red puede consistir en dos sistemas finales que necesitan comunicarse sin estar conectados a la misma red. Más bien, supondremos que están conectados a redes que, directa o indirectamente, están conectadas entre sí. Este caso requiere el uso de alguna técnica de interconexión entre redes. Estas técnicas se estudiarán en el Capítulo 18.

Capa de transporte

La capa de transporte proporciona un mecanismo para intercambiar datos entre sistemas finales. El servicio de transporte orientado a conexión asegura que los datos se entregan libres de errores, en orden y sin pérdidas ni duplicaciones. La capa de transporte también puede estar involucrada en la optimización del uso de los servicios de red, y en proporcionar la calidad del servicio solicitada. Por ejemplo, la entidad de sesión puede solicitar una tasa máxima de error determinada, un retardo máximo, una prioridad y un nivel de seguridad dado.

El tamaño y la complejidad de un protocolo de transporte dependen de cómo de fiables sean los servicios de red y las redes subyacentes. Consecuentemente, ISO ha desarrollado una familia de cinco protocolos de transporte normalizados, cada uno de ellos especificado para un determinado servicio subyacente. En la arquitectura de protocolos TCP/IP se han especificado dos protocolos para la capa de transporte: el orientado a conexión, TCP (Protocolo de Control de la Transmisión, *Transmission Control Protocol*) y el no orientado a conexión UDP (Protocolo de Datagrama de Usuario, *User Datagram Protocol*).

Capa de sesión

Las cuatro capas inferiores del modelo OSI proporcionan un medio para el intercambio fiable de datos permitiendo, a su vez, distintos niveles de calidad de servicio. Para muchas aplicaciones, este servicio básico es, a todas luces, insuficiente. Por ejemplo, una aplicación de acceso a un terminal remoto puede requerir un diálogo *half-duplex*. Por el contrario, una aplicación para el procesamiento de transacciones puede necesitar la inclusión de puntos de comprobación en el flujo de transferencia para poder hacer operaciones de respaldo y recuperación. De igual manera, otra aplicación para procesar mensajes puede requerir la posibilidad de interrumpir el diálogo, generar nuevos mensajes y, posteriormente, continuar el diálogo desde donde se interrumpió.

Todas estas capacidades se podrían incorporar en las aplicaciones de la capa 7. Sin embargo, ya que todas estas herramientas para el control del diálogo son ampliamente aplicables, parece lógico organizarlas en una capa separada, denominada capa de sesión.

La capa de sesión proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles. No obstante, en algunas aplicaciones su utilización es ineludible. La capa de sesión proporciona los siguientes servicios:

- **Control del diálogo:** éste puede ser simultáneo en los dos sentidos (*full-duplex*) o alternado en ambos sentidos (*half-duplex*).
- **Agrupamiento:** el flujo de datos se puede marcar para definir grupos de datos. Por ejemplo, si una empresa o almacén está transmitiendo los datos correspondientes a las ventas hacia una oficina regional, éstos se pueden marcar de tal manera que se indique por grupos el final de las ventas realizadas en cada departamento. Este servicio permitiría que el computador destino calcule los totales de las ventas realizadas en cada departamento.
- **Recuperación:** la capa de sesión puede proporcionar un procedimiento de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación.

ISO ha definido una normalización para la capa de sesión que incluye como opciones los servicios que se acaban de describir.

Capa de presentación

La capa de presentación define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. La capa de presentación define la sintaxis utilizada entre las entidades de aplicación y proporciona los medios para seleccionar y modificar la representación utilizada. Algunos ejemplos de servicios específicos que se pueden realizar en esta capa son los de compresión y cifrado de datos.

Capa de aplicación

La capa de aplicación proporciona a los programas de aplicación un medio para que accedan al entorno OSI. A esta capa pertenecen las funciones de administración y los mecanismos genéricos necesarios para la implementación de aplicaciones distribuidas. Además, en esta capa también residen las aplicaciones de uso general como, por ejemplo, la transferencia de archivos, el correo electrónico y el acceso desde terminales a computadores remotos, entre otras.

2.4. LA ARQUITECTURA DE PROTOCOLOS TCP/IP

La arquitectura de protocolos TCP/IP es resultado de la investigación y desarrollo llevados a cabo en la red experimental de conmutación de paquetes ARPANET, financiada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA, *Defense Advanced Research Projects Agency*), y se denomina globalmente como la familia de protocolos TCP/IP. Esta familia consiste en una extensa colección de protocolos que se han especificado como estándares de Internet por parte de IAB (*Internet Architecture Board*).

LAS CAPAS DE TCP/IP

El modelo TCP/IP estructura el problema de la comunicación en cinco capas relativamente independientes entre sí:

- Capa física.
- Capa de acceso a la red.
- Capa internet.
- Capa extremo-a-extremo o de transporte.
- Capa de aplicación.

La **capa física** define la interfaz física entre el dispositivo de transmisión de datos (por ejemplo, la estación de trabajo o el computador) y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos y cuestiones afines.

La **capa de acceso a la red** es responsable del intercambio de datos entre el sistema final (servidor, estación de trabajo, etc.) y la red a la cual está conectado. El emisor debe proporcionar a la red la dirección del destino, de tal manera que ésta pueda encaminar los datos hasta el destino apropiado. El emisor puede requerir ciertos servicios que pueden ser proporcionados por el nivel de red, por ejemplo, solicitar una determinada prioridad. El software en particular que se use en esta capa dependerá del tipo de red que se disponga. Así, se han desarrollado, entre otros, diversos estándares para la conmutación de circuitos, la conmutación de paquetes (por ejemplo, retransmisión de tramas) y para las redes de área local (por ejemplo, Ethernet). Por tanto, tiene sentido separar en una capa diferente todas aquellas funciones que tengan que ver con el acceso a la red. Haciendo esto, el software de comunicaciones situado por encima de la capa de acceso a la red no tendrá que ocuparse de los detalles específicos de la red a utilizar. El software de las capas superiores debería, por tanto, funcionar correctamente con independencia de la red a la que el computador esté conectado.

Para sistema finales conectados a la misma red, la capa de acceso a la red está relacionada con el acceso y encaminamiento de los datos. En situaciones en las que los dos dispositivos estén conectados a redes diferentes, se necesitarán una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas. Ésta es la función de la **capa internet**. El protocolo internet (IP, *Internet Protocol*) se utiliza en esta capa para ofrecer el servicio de encaminamiento a través de varias redes. Este protocolo se implementa tanto en los sistemas finales como en los encaminadores intermedios. Un encaminador es un procesador que conecta dos redes y cuya función principal es retransmitir datos desde una red a otra siguiendo la ruta adecuada para alcanzar al destino.

Independientemente de la naturaleza de las aplicaciones que estén intercambiando datos, es usual requerir que los datos se intercambien de forma fiable. Esto es, sería deseable asegurar que todos los datos llegan a la aplicación destino y en el mismo orden en el que fueron enviados. Como se estudiará más adelante, los mecanismos que proporcionan esta fiabilidad son esencialmente independientes de la naturaleza intrínseca de las aplicaciones. Por tanto, tiene sentido agrupar todos estos mecanismos en una capa común compartida por todas las aplicaciones; ésta se denomina **capa extremo-a-extremo**, o **capa de transporte.** El protocolo para el control de la transmisión, TCP (*Transmission Control Protocol*), es el más utilizado para proporcionar esta funcionalidad.

Finalmente, la **capa de aplicación** contiene toda la lógica necesaria para posibilitar las distintas aplicaciones de usuario. Para cada tipo particular de aplicación, como por ejemplo, la transferencia de archivos, se necesitará un módulo bien diferenciado.

La Figura 2.12 muestra las capas de las arquitecturas OSI y TCP/IP, indicando la posible correspondencia en términos de funcionalidad entre ambas.

TCP Y UDP

La mayor parte de aplicaciones que se ejecutan usando la arquitectura TCP/IP usan como protocolo de transporte TCP. TCP proporciona una conexión fiable para transferir los datos entre las aplicaciones. Una conexión es simplemente una asociación lógica de carácter temporal entre dos entidades de sistemas distintos. Cada PDU de TCP, denominada **segmento TCP**, contiene en la cabecera la identificación de los puertos origen y destino, los cuales corresponden con los puntos de acceso al servicio (SAP) de la arquitectura OSI. Los valores de los puertos identifican a los respectivos usuarios (aplicaciones) de las dos entidades TCP. Una conexión lógica alude a un par de puertos. Durante la conexión, cada entidad seguirá la pista de los segmentos TCP que vengan y vayan hacia la otra entidad, para así regular el flujo de segmentos y recuperar aquellos que se pierdan o dañen.

Además del protocolo TCP, la arquitectura TCP/IP usa otro protocolo de transporte: el protocolo de datagramas de usuario, UDP (*User Datagram Protocol*). UDP no garantiza la entrega, la

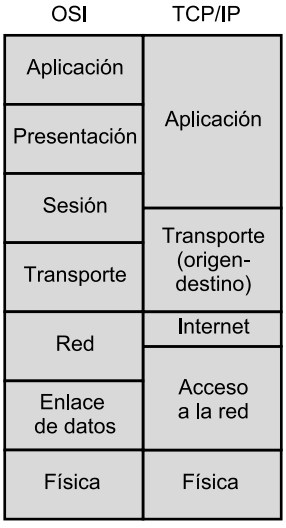


Figura 2.12. Comparación entre las arquitecturas de protocolos TCP/IP y OSI.

conservación del orden secuencial, ni la protección frente duplicados. UDP posibilita el envío de mensajes entre aplicaciones con la complejidad mínima. Algunas aplicaciones orientadas a transacciones usan UDP. Un ejemplo es SNMP (*Simple Network Management Protocol*), el protocolo normalizado para la gestión en las redes TCP/IP. Debido a su carácter no orientado a conexión, UDP en realidad tiene poca tarea que hacer. Básicamente, su cometido es añadir a IP la capacidad de identificar los puertos.

FUNCIONAMIENTO DE TCP E IP

La Figura 2.13 muestra cómo se configuran los protocolos TCP/IP. Para poner de manifiesto que el conjunto total de recursos para la comunicación puede estar formado por varias redes, a dichas redes constituyentes se les denomina **subredes**. Para conectar un computador a una subred se utiliza algún tipo de protocolo de acceso, por ejemplo, Ethernet. Este protocolo permite al computador enviar datos a través de la subred a otro computador o, en caso de que el destino final esté en otra subred, a un dispositivo de encaminamiento que los retransmitirá. IP se implementa en todos los sistemas finales y dispositivos de encaminamiento. Actúa como un porteador que transportara bloques de datos desde un computador hasta otro, a través de uno o varios dispositivos de encaminamiento. TCP se implementa solamente en los sistemas finales, donde supervisa los bloques de datos para asegurar que todos se entregan de forma fiable a la aplicación apropiada.

Para tener éxito en la transmisión, cada entidad en el sistema global debe tener una única dirección. En realidad, se necesitan dos niveles de direccionamiento. Cada computador en una subred dada debe tener una dirección de internet única que permita enviar los datos al computador adecuado. Además, cada proceso que se ejecute dentro de un computador dado debe tener, a su vez,

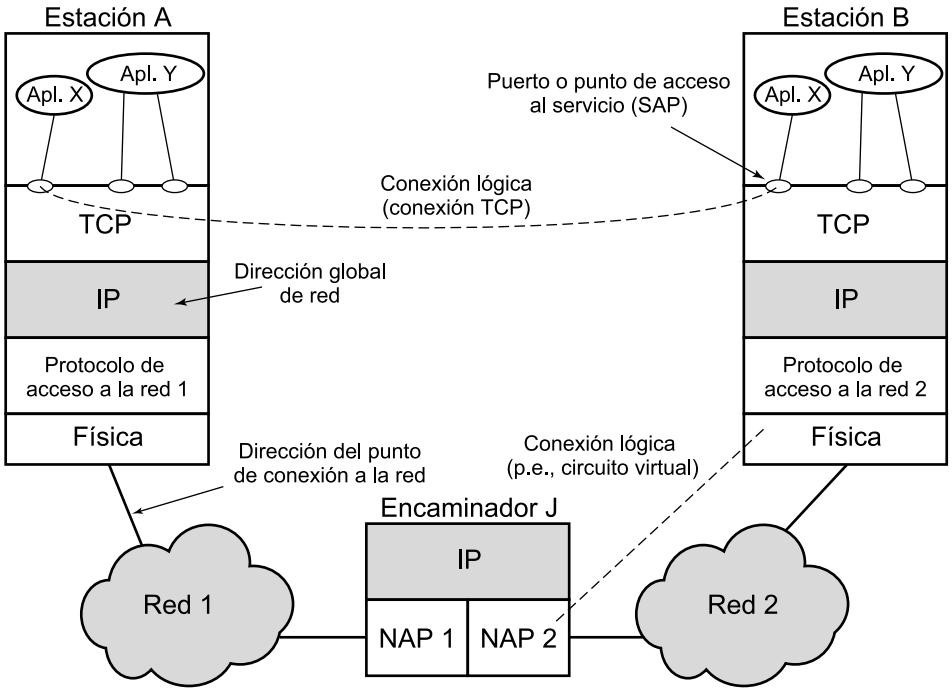


Figura 2.13. Conceptos de TCP/IP.

una dirección que sea única dentro del mismo. Esto permite al protocolo extremo-a-extremo (TCP) entregar los datos al proceso adecuado. Estas últimas direcciones se denominan puertos.

A continuación se va a describir paso a paso un sencillo ejemplo. Supóngase que un proceso, asociado al puerto 1 en el computador A, desea enviar un mensaje a otro proceso, asociado al puerto 2 del computador B. El proceso en A pasa el mensaje a TCP con la instrucción de enviarlo al puerto 2 del computador B. TCP pasa el mensaje a IP con la instrucción de enviarlo al computador B. Obsérvese que no es necesario comunicarle a IP la identidad del puerto destino. Todo lo que necesita saber es que los datos van dirigidos al computador B. A continuación, IP pasa el mensaje a la capa de acceso a la red (por ejemplo, a la lógica de Ethernet) con el mandato expreso de enviarlo al dispositivo de encaminamiento J (el primer salto en el camino hacia B).

Para controlar esta operación se debe transmitir información de control junto con los datos de usuario, como así se sugiere en la Figura 2.14. Supongamos que el proceso emisor genera un bloque de datos y lo pasa a TCP. TCP puede que divida este bloque en fragmentos más pequeños para hacerlos más manejables. A cada uno de estos fragmentos le añade información de control, denominada cabecera TCP, formando un **segmento TCP**. La información de control la utilizará la entidad par TCP en el computador B. Entre otros, en la cabecera se incluyen los siguientes campos:

- **Puerto destino:** cuando la entidad TCP en B recibe el segmento, debe conocer a quién se le deben entregar los datos.
- **Número de secuencia:** TCP numera secuencialmente los segmentos que envía a un puerto destino dado para que, si llegan desordenados, la entidad TCP en B pueda reordenarlos.
- **Suma de comprobación:** la entidad emisora TCP incluye un código calculado en función del resto del segmento. La entidad receptora TCP realiza el mismo cálculo y compara el resultado con el código recibido. Si se observa alguna discrepancia implicará que ha habido algún error en la transmisión.

A continuación, TCP pasa cada segmento a IP con instrucciones para que los transmita a B. Estos segmentos se transmitirán a través de una o varias subredes y serán retransmitidos en uno

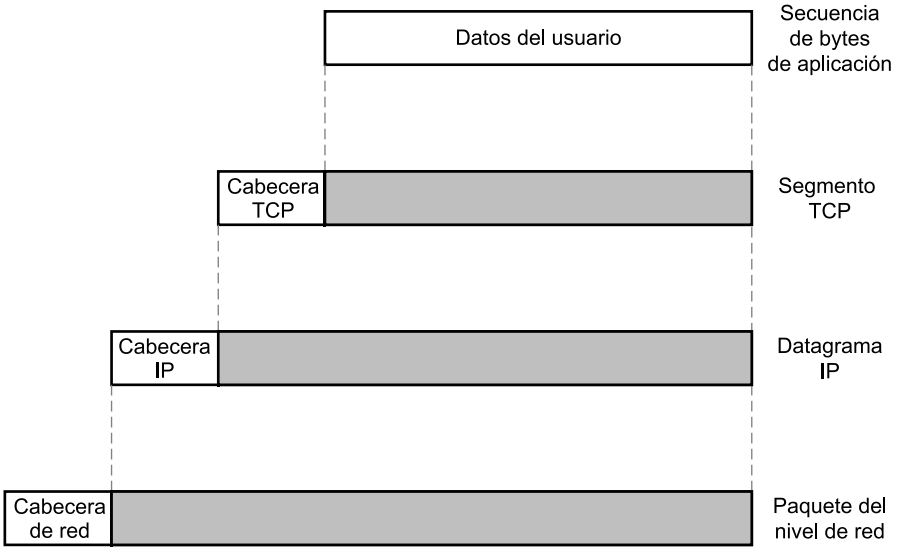


Figura 2.14. Unidades de datos de protocolo en la arquitectura TCP/IP.

o más dispositivos de encaminamiento intermedios. Esta operación también requiere el uso de información de control. Así, IP añade una cabecera de información de control a cada segmento para formar lo que se denomina un **datagrama IP**. En la cabecera IP, además de otros campos, se incluirá la dirección del computador destino (en nuestro ejemplo B).

Finalmente, cada datagrama IP se pasa a la capa de acceso a la red para que se envíe a través de la primera subred. La capa de acceso a la red añade su propia cabecera, creando un paquete, o trama. El paquete se transmite a través de la subred al dispositivo de encaminamiento J. La cabecera del paquete contiene la información que la subred necesita para transferir los datos. La cabecera puede contener, entre otros, los siguientes campos:

- **Dirección de la subred destino**: la subred debe conocer a qué dispositivo se debe entregar el paquete.
- **Funciones solicitadas**: el protocolo de acceso a la red puede solicitar la utilización de ciertas funciones ofrecidas por la subred, por ejemplo, la utilización de prioridades.

En el dispositivo de encaminamiento J, la cabecera del paquete se elimina y, posteriormente, se examina la cabecera IP. El módulo IP del dispositivo de encaminamiento direcciona el paquete a través de la subred 2 hacia B basándose en la dirección destino que contenga la cabecera IP. Para hacer esto, se le añade al datagrama una cabecera de acceso a la red.

Cuando se reciben los datos en B, ocurre el proceso inverso. En cada capa se elimina la cabecera correspondiente y el resto se pasa a la capa inmediatamente superior, hasta que los datos de usuario originales alcancen al proceso destino.

Como nota final, recuérdese que el nombre genérico del bloque de datos intercambiado en cualquier nivel se denomina **unidad de datos del protocolo** (PDU, *Protocol Data Unit*). Consecuentemente, el segmento TCP es la PDU del protocolo TCP.

APLICACIONES TCP/IP

Se han normalizado una serie de aplicaciones para funcionar por encima de TCP. A continuación se mencionan tres de las más importantes.

El **protocolo simple de transferencia de correo (SMTP, *Simple Mail Transfer Protocol*)** proporciona una función básica de correo electrónico. Este protocolo establece un mecanismo para transferir mensajes entre computadores remotos. Entre las características de SMTP cabe destacar la utilización de listas de mensajería, la gestión de acuses de recibo y el reenvío de mensajes. El protocolo SMTP no especifica cómo se crean los mensajes. Para este fin se necesita un programa de correo electrónico nativo o un editor local. Una vez que se ha creado el mensaje, SMTP lo acepta y, utilizando TCP, lo envía al módulo SMTP del computador remoto. En el receptor, el módulo SMTP utilizará su aplicación de correo electrónico local para almacenar el mensaje recibido en el buzón de correo del usuario destino.

El **protocolo de transferencia de archivos (FTP, *File Transfer Protocol*)** se utiliza para enviar archivos de un sistema a otro bajo el control del usuario. Se permite transmitir archivos tanto de texto como en binario. Además, el protocolo permite controlar el acceso de los usuarios. Cuando un usuario solicita la transferencia de un archivo, FTP establece una conexión TCP con el sistema destino para intercambiar mensajes de control. Esta conexión permite al usuario transmitir su identificador y contraseña, además de la identificación del archivo junto con las acciones a realizar sobre el mismo. Una vez que el archivo se haya especificado y su transferencia haya sido aceptada, se establecerá una segunda conexión TCP a través de la cual se materializará la transferencia. El

archivo se transmite a través de la segunda conexión, sin necesidad de enviar información extra o cabeceras generadas por la capa de aplicación. Cuando la transferencia finaliza, se utiliza la conexión de control para indicar la finalización. Además, esta misma conexión estará disponible para aceptar nuevas órdenes de transferencia.

TELNET facilita la realización de conexiones remotas, mediante las cuales el usuario en un terminal o computador personal se conecta a un computador remoto y trabaja como si estuviera conectado directamente a ese computador. El protocolo se diseñó para trabajar con terminales poco sofisticados en modo *scroll* (avance de pantalla). En realidad, TELNET se implementa en dos módulos: el usuario TELNET interactúa con el módulo de E/S para comunicarse con un terminal local. Este convierte las particularidades de los terminales reales a una definición normalizada de terminal de red y viceversa. El servidor TELNET interactúa con la aplicación, actuando como un sustituto del gestor del terminal, para que de esta forma el terminal remoto le parezca local a la aplicación. El tráfico entre el terminal del usuario y el servidor TELNET se lleva a cabo sobre una conexión TCP.

INTERFACES DE PROTOCOLO

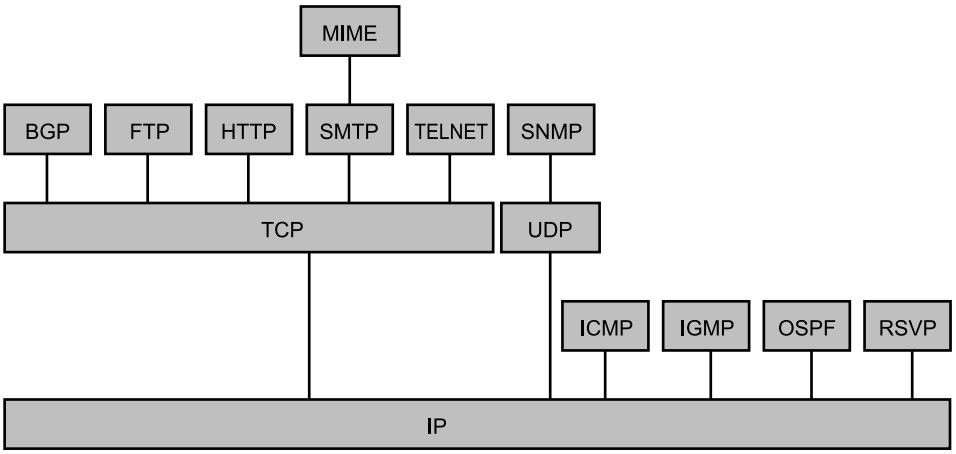
En la familia de protocolos TCP/IP cada capa interacciona con sus capas inmediatamente adyacentes. En el origen, la capa de aplicación utilizará los servicios de la capa extremo-a-extremo, pasándole los datos. Este procedimiento se repite en la interfaz entre la capa extremo-a-extremo y la capa internet, e igualmente en la interfaz entre la capa internet y la capa de acceso a la red. En el destino, cada capa entrega los datos a la capa superior adyacente.

La arquitectura de TCP/IP no exige que se haga uso de todas las capas. Como así se sugiere en la Figura 2.15, es posible desarrollar aplicaciones que invoquen directamente los servicios de cualquier capa. La mayoría de las aplicaciones requieren un protocolo extremo-a-extremo fiable y, por tanto, utilizan TCP. Otras aplicaciones de propósito específico no necesitan de los servicios del TCP. Algunas de estas, por ejemplo, el protocolo simple de gestión de red (SNMP), utilizan un protocolo extremo-a-extremo alternativo denominado protocolo de datagrama de usuario (UDP); otras, en cambio, incluso pueden usar el protocolo IP directamente. Las aplicaciones que no necesiten interconexión de redes y que no necesiten TCP pueden invocar directamente los servicios de la capa de acceso a la red.

2.5. LECTURAS RECOMENDADAS Y SITIOS WEB

Para el lector que esté interesado en profundizar en el estudio de TCP/IP, hay dos trabajos de tres volúmenes cada uno muy adecuados. Los trabajos de Comer y Stevens se han convertido en un clásico y son considerados como definitivos [COME00, COME99, COME01]. Los trabajos de Stevens y Wright son igualmente dignos de mención y más explícitos en la descripción del funcionamiento de los protocolos [STEV94, STEV96, WRIG95]. Un libro más compacto y útil como manual de referencia es [RODR02], en el que se cubre todo el espectro de protocolos relacionados con TCP/IP de una forma concisa y elegante, incluyendo la consideración de algunos protocolos no estudiados en los otros dos trabajos.

COME99 Comer, D., y Stevens, D. *Internetworking with TCP/IP, Volume II: Design Implementation, and Internals.* Upper Saddle River, NJ: Prentice Hall, 1994.



BGP (*Border gateway protocol*) = Protocolo de pasarela fronteriza
FTP (*File transfer protocol*) = Protocolo de transferencia de archivos
HTTP (*Hypertext transfer protocol*) = Protocolo de transferencia de hipertexto
ICMP (*Internet control message protocol*) = Protocolo de mensajes de control de Internet
IGMP (*Internet group management protocol*) = Protocolo de gestión de grupos en Internet
IP (*Internet protocol*) = Protocolo Internet
MIME (*Multipurpose internet mail extension*) = Extensiones multipropósito de correo electrónico
OSPF (*Open shortest path first*) = Protocolo del primer camino más corto disponible
RSVP (*Resource reservation protocol*) = Protocolo de reserva de recursos
SMTP (*Simple mail transfer protocol*) = Protocolo simple de transferencia de correo electrónico
SNMP (*Simple network management protocol*) = Protocolo simple de gestión de red
TCP (*Transmission control protocol*) = Protocolo de control de transmisión
UDP (*User datagram protocol*) = Protocolo de datagrama de usuario

Figura 2.15. Algunos protocolos en la familia de protocolos TCP/IP.

COME00 Comer D. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture.* Upper Saddle River, NJ: Prentice Hall, 2000.

COME01 Comer, D., y Stevens, D. *Internetworking with TCP/IP, Volume III: Client-Server Programming and Applications.* Upper Saddle River, NJ: Prentice Hall, 2001.

RODR02 Rodríguez, A., et al., *TCP/IP: Tutorial and Technical Overview.* Upper Saddle River: NJ: Prentice Hall, 2002.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols.* Reading, MA: Addison-Wesley, 1994.

STEV96 Stevens, W. *TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX(R) Domain Protocol.* Reading, MA: Addison-Wesley, 1996.

WRIG95 Wright, G., y Stevens, W. *TCP/IP Illustrated*, *Volume* 2: *The Implementation*. Reading, MA: Addison-Wesley, 1995.

SITIO WEB RECOMENDADO

- **«Networking Links»:** ofrece una excelente colección de enlaces relacionadas con TCP/IP.

2.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

arquitectura de protocolos
cabecera
capa de aplicación
capa de presentación
capa de red
capa de sesión
capa de transporte
capa de enlace de datos
capa física
capa par
dispositivo de encaminamiento o encaminador
interconexión de redes
interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*)
Internet
protocolo
protocolo de control de transmisión (TCP, *Transmission Control Protocol*)
protocolo de datagramas de usuario (UDP, *User Datagram Protocol*)
protocolo internet (IP, *Internet Protocol*)
puerto
punto de acceso al servicio (SAP, *Service Access Point*)
subred
suma de comprobación
unidad de datos del protocolo (PDU, *Protocolo Data Unit*)

CUESTIONES DE REPASO

2.1 ¿Cuál es la función principal de la capa de acceso a la red?

2.2. ¿Qué tareas realiza la capa de transporte?

2.3. ¿Qué es un protocolo?

2.4. ¿Qué es una unidad de datos del protocolo (PDU)?

2.5. ¿Qué es una arquitectura de protocolos?

2.6. ¿Qué es TCP/IP?

2.7. ¿Qué ventajas aporta una arquitectura en capas como la usada en TCP/IP?

2.8. ¿Qué es un encaminador?

EJERCICIOS

2.1. Usando los modelos de capas de la Figura 2.16, describa el procedimiento de pedir y enviar una pizza, indicando las interacciones habidas en cada nivel.

2.2. **a)** Los primeros ministros de China y Francia necesitan alcanzar un acuerdo por teléfono, pero ninguno de los dos habla el idioma de su interlocutor. Es más, ninguno tiene cerca un traductor que traduzca el idioma del otro. No obstante, ambos tienen un traductor de inglés. Dibuje un diagrama similar al de la Figura 2.16 que describa la situación y detalle las interacciones que haya en cada nivel.

b) Suponga ahora que el traductor del primer ministro chino puede traducir sólo al japonés y que el primer ministro francés tiene un traductor alemán. Un traductor de japonés a alemán se encuentra disponible en Alemania. Dibuje el diagrama que refleje esta nueva situación y describa la hipotética conversación telefónica.

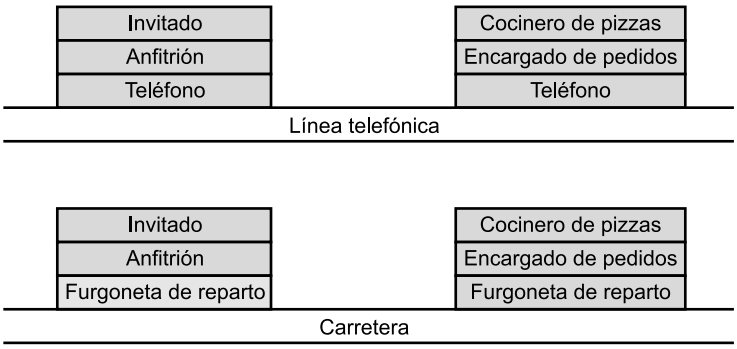


Figura 2.16. Arquitectura del Ejercicio 2.1.

2.3. Enumere las desventajas del diseño en capas para los protocolos.

2.4. Dos cuerpos de ejército (de color azul), situados sobre dos colinas, están preparando un ataque a un único ejército (de color rojo) situado en el valle que las separa. El ejército rojo puede vencer por separado a cada cuerpo del ejército azul, pero fracasará si los dos ejércitos azules le atacan simultáneamente. Los cuerpos de ejército azules se comunican mediante un sistema de comunicación no fiable (un soldado de infantería). El comandante de uno de los cuerpos de ejército azul desearía atacar al mediodía. Su problema es éste: si envía un mensaje ordenando el ataque, no puede estar seguro de que el mensaje haya llegado. Podría solicitar una confirmación, pero ésta también podría ser interceptada. ¿Existe algún protocolo que pueda utilizar el ejército azul para evitar la derrota?

2.5. Una red de difusión es aquella en la que las transmisiones de cualquier estación son recibidas por todas las estaciones conectadas al medio compartido. Ejemplos son una red de área local con topología en *bus*, como Ethernet, o una red inalámbrica. Discuta si es necesaria o no una capa de red (capa 3 de OSI) en una red de difusión.

2.6 Basándose en los principios enunciados en la Tabla 2.1:

a) Diseñe una arquitectura con ocho capas y ponga un ejemplo de su utilización.

b) Diseñe otra con seis capas y ponga otro ejemplo para ésta.

2.7. En la Figura 2.14, la unidad de datos del protocolo (PDU) de la capa N se encapsula en una PDU de la capa $(N - 1)$. Igualmente, se puede partir la PDU del nivel N en varias PDU del nivel $(N - 1)$ (segmentación) o agrupar varias PDU del nivel N en una única PDU del nivel $(N - 1)$ (agrupamiento).

a) En la segmentación, ¿es necesario que cada segmento del nivel $(N - 1)$ contenga una copia de la cabecera del nivel N?

b) En el agrupamiento, ¿es necesario que cada una de las PDU conserve su cabecera o se pueden agrupar los datos en una única PDU de nivel N con una única cabecera de nivel N?

2.8. La versión anterior de la especificación del protocolo TFTP, RFC 783, decía:

«Todos los paquetes, exceptuando aquellos utilizados para terminar, se confirman individualmente a menos que el temporizador correspondiente expire.»

El RFC 1350 modificó esta frase para decir:

«Todos los paquetes, exceptuando los ACK (confirmaciones, del inglés *ACKnowledgement*) duplicados y los utilizados para terminar, se confirman a menos que el correspondiente temporizador expire.»

Este cambio se ha introducido para corregir el problema denominado del «aprendiz de brujo». Deduzca y explique el problema.

2.9. ¿Cuál es el factor que determina el tiempo necesario para transferir un archivo usando TFTP?

APÉNDICE 2A. EL PROTOCOLO TFTP (*TRIVIAL FILE TRANSFER PROTOCOL*)

En este apéndice se proporciona un resumen de la norma protocolo trivial para la transferencia de archivos (TFTP, *Trivial File Transfer Protocol*) de Internet, definido en el RFC 1350. Nuestro propósito aquí es ilustrar al lector sobre el uso de los elementos de un protocolo.

INTRODUCCIÓN A TFTP

TFTP es mucho más sencillo que la norma de Internet FTP (RFC 959). No hay mecanismos para controlar el acceso o la identificación de los usuarios. Por tanto, TFTP está sólo indicado para acceder a directorios públicos. Debido a su simplicidad, TFTP se implementa fácilmente y de una forma compacta. Por ejemplo, algunos dispositivos sin discos utilizan TFTP para descargar el código ejecutable para arrancar.

TFTP se ejecuta por encima de UDP. La entidad TFTP que inicia la transferencia lo hace enviando una solicitud de lectura o escritura en un segmento UDP al puerto 69 del destino. Este puerto se reconoce por parte del módulo UDP como el identificador del módulo TFTP. Mientras dura la transferencia, cada extremo utiliza un identificador para la transferencia (TID, *Transfer identifier*) como su número de puerto.

PAQUETES TFTP

Las entidades TFTP intercambian órdenes, respuestas y datos del archivo mediante paquetes, cada uno de los cuales se transporta en el cuerpo de un segmento UDP. TFTP considera cinco tipos de paquetes (*véase* Figura 2.17); los dos primeros bytes contienen un código que identifica el tipo de paquete de que se trata:

- **RRQ (*Read ReQuest packet*):** paquete para solicitar permiso para leer un archivo desde el otro sistema. Este paquete indica el nombre del archivo en una secuencia de bytes en ASCII[3] terminada por un byte cero. Con este byte cero se indica a la entidad TFTP receptora que el nombre del archivo ha concluido. Este paquete también incluye un campo denominado modo, el cual indica cómo ha de interpretarse el archivo de datos: como una cadena de bytes ASCII o como datos de 8 bits en binario.

[3] ASCII es la norma *American Standard Code for Information Interchange* especificada por el *American Standards Institute*. Asigna un patrón único de 7 bits a cada letra, usando el bit octavo como paridad. ASCCI es equivalente al alfabeto de referencia internacional (IRA, *Internacional Referente Alphabet*), definido por la UIT-T en la recomendación T.50.

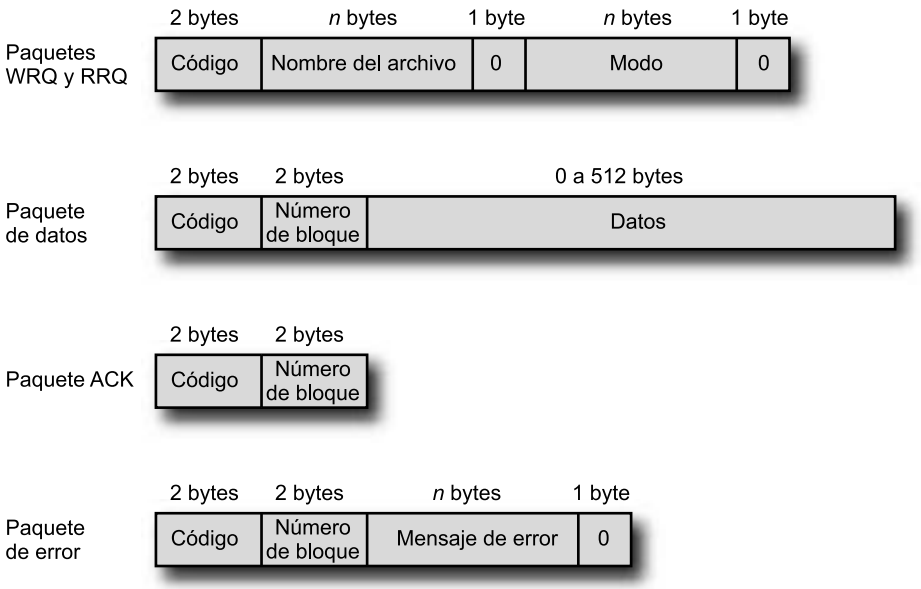


Figura 2.17. Formatos de los paquetes TFTP.

- **WRQ (*Write ReQuest packet*):** paquete para solicitar permiso para enviar un archivo al otro sistema.
- **Datos:** los bloques de datos se empiezan a enumerar desde uno y se incrementa su numeración por cada nuevo bloque de datos. Esta convención posibilita que el programa use un número para discriminar entre paquetes nuevos y duplicados. El campo de datos tiene una longitud entre cero y 512 bytes. Cuando es de 512 bytes, se interpreta como que no es el último bloque de datos. Cuando su longitud está comprendida entre cero y 511, indica el final de la transferencia.
- **ACK (*Acknowledgement*):** este paquete confirma la recepción de un paquete WRQ o de datos. El ACK de un paquete de datos contiene el número de bloque del paquete de datos confirmado. Un ACK de un WRQ contendrá un número de bloque igual a cero.
- **Error:** estos paquetes pueden corresponder a la confirmación de cualquier tipo de paquete. El código de error es un entero que indica la naturaleza del error (Tabla 2.4). El mensaje de error está destinado a ser interpretado por un humano, debiendo ser código ASCII. Al igual que todas las otras cadenas, se delimita finalmente con un byte cero.

Todos los paquetes, excepto los ACK duplicados (posteriormente explicados) y los usados para finalizar, tienen que ser confirmados. Para cualquier paquete se puede devolver un paquete de error. Si no hay errores, se aplica el siguiente convenio: los paquetes de datos o de tipo WRQ se confirman con un paquete ACK. Cuando se envía un RRQ, el otro extremo debe responder (siempre que no haya error) transmitiendo el archivo; por tanto, el primer bloque de datos sirve como confirmación del paquete RRQ. Hasta que no se concluya la transferencia del archivo, cada paquete ACK generado será seguido por un paquete de datos en el otro sentido. De esta forma los paquetes de datos sirven igualmente como confirmaciones. Un paquete de error podrá ser confirmado por cualquier tipo de paquete, dependiendo de las circunstancias.

Tabla 2.4. Códigos de error en TFTP.

Valor	Significado
0	No definido, ver mensaje de error (si lo hubiera)
1	Archivo no encontrado
2	Fallo en el acceso
3	Disco lleno o cuota excedida
4	Operación TFTP no válida
5	TID desconocido
6	El archivo ya existe
7	Usuario no existente

EJEMPLO DE TRANSFERENCIA

El ejemplo que se muestra en la Figura 2.18 corresponde a una transferencia sencilla desde A a B. Se supone que no ocurren errores. Es más, en la figura no se muestran los detalles acerca de la especificación de las opciones.

La operación comienza cuando el módulo TFTP del sistema A envía una solicitud de escritura (WRQ) al módulo TFTP del sistema B. El paquete WRQ se transporta en el cuerpo de un segmento UDP. La solicitud de escritura incluye el nombre del archivo (en el ejemplo XXX) y un octeto que indica el modo, binario u octetos. En la cabecera UDP, el puerto destino es el 69, el cual avisa a la entidad UDP receptora que el mensaje está dirigido a la aplicación de TFTP. El número del puerto origen es un TID seleccionado por A, en el ejemplo 1511. El sistema B está preparado para aceptar el archivo. Por tanto, devuelve un ACK con número de bloque 0. En la cabecera UDP, el puerto destino es 1511, el cual habilita a la entidad UDP en A a encaminar el paquete recibido al módulo TFTP, el cual podrá cotejar este TID con el TID del WRQ. El puerto origen es un TID seleccionado por B para la transferencia del archivo, 1660 en el ejemplo.

Siguiendo con el ejemplo, se procede a la transferencia del archivo. El envío consiste en uno o más paquetes desde A, cada uno de los cuales ha de ser confirmado por B. El último paquete de datos contiene menos de 512 bytes de datos, lo que indica el fin de la transferencia.

ERRORES Y RETARDOS

Si TFTP funciona sobre una red o sobre una internet (por oposición a un enlace directo de datos), es posible que ciertos paquetes se pierdan. Debido a que TFTP funciona sobre UDP, el cual no proporciona un servicio con entrega garantizada, se necesita en TFTP un mecanismo que se encargue de tratar con estos posibles paquetes perdidos. En TFTP se usa una técnica habitual basada en expiración de temporizadores. Supóngase que A envía un paquete a B que requiere ser confirmado. (es decir, cualquier paquete que no sea un ACK duplicado o uno utilizado para terminar). Cuando A envía el paquete, inicia un temporizador. Si el temporizador expira antes de que se reciba de B

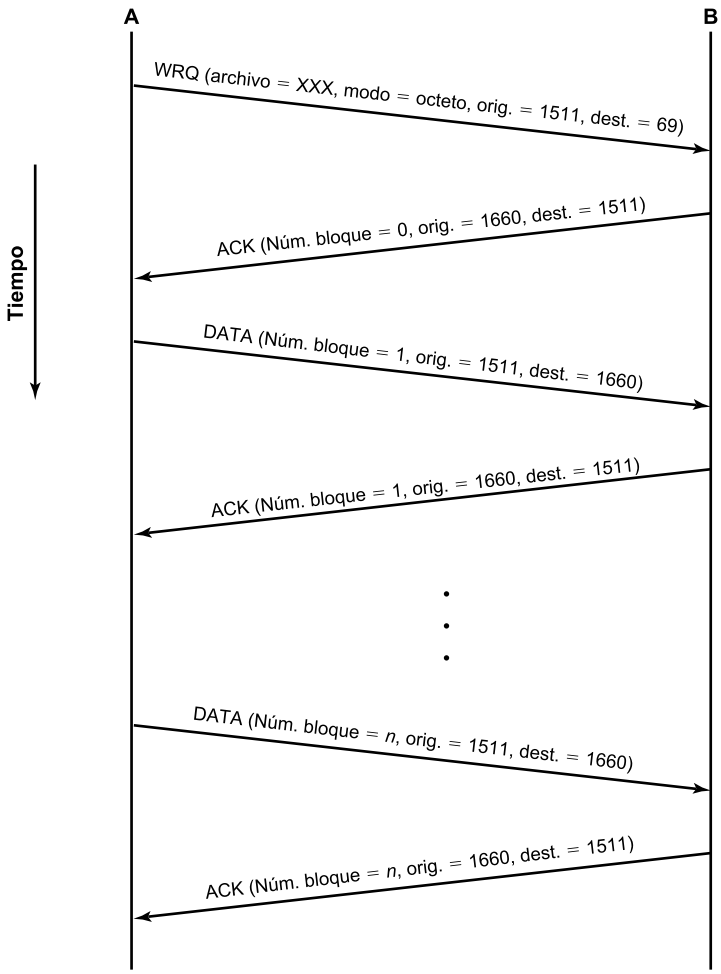

A
B
WRQ (archivo = XXX, modo = octeto, orig. = 1511, dest. = 69)
ACK (Núm. bloque = 0, orig. = 1660, dest. = 1511)
Tiempo
DATA (Núm. bloque = 1, orig. = 1511, dest. = 1660)
ACK (Núm. bloque = 1, orig. = 1660, dest. = 1511)
DATA (Núm. bloque = n, orig. = 1511, dest. = 1660)
ACK (Núm. bloque = n, orig. = 1660, dest. = 1511)

Figura 2.18. Ejemplo de funcionamiento de TFTP.

la confirmación, A retransmitirá el mismo paquete anterior. Si de hecho el paquete original se perdió, la retransmisión será la primera instancia del paquete que reciba B. Si el paquete original no se perdió, pero sí la confirmación de B, B recibirá dos copias del mismo paquete, confirmando ambas. Debido al uso de número de bloques, esta última contingencia no introducirá confusión alguna. La única excepción sería el caso de ACK duplicados. En este caso, el segundo ACK se ignorará.

SINTAXIS, SEMÁNTICA Y TEMPORIZACIÓN

En el Apartado 2.1 se mencionó que las características o aspectos clave de cualquier protocolo se pueden clasificar en sintaxis, semántica y temporización. Estas categorías se pueden identificar fácilmente en TFTP. El formato de los distintos paquetes TFTP constituye la **sintaxis** del protocolo. La **semántica** del protocolo consiste en las definiciones de cada uno de los tipos de paquetes y códigos de error. Finalmente, el orden en que se intercambian los paquetes, la numeración de los bloques y el uso de temporizadores son todos ellos aspectos relativos a la **temporización** de TFTP.

PARTE II

COMUNICACIONES DE DATOS

CUESTIONES DE LA PARTE II

En la Parte II se estudia la transferencia de datos entre dos dispositivos que estén directamente conectados; es decir, dos dispositivos que estén enlazados por medio de un único camino y no por una red. Incluso en este contexto tan restringido, hay una cantidad considerable de cuestiones técnicas y de diseño a analizar. En primer lugar, es necesario conocer cómo se transmiten las señales a través del enlace de comunicación. En la transmisión, se utilizarán tanto técnicas analógicas como digitales. En ambos casos, las señales se considerarán que están formadas por un conjunto de componentes espectrales definidas en un rango de frecuencias electromagnéticas. Las propiedades de transmisión de la señal dependerán de las frecuencias involucradas. Igualmente, en la transmisión, los defectos y limitaciones que sufra la señal, por ejemplo la atenuación, dependerán de la frecuencia. Un aspecto independiente de los anteriores es el propio medio que se utilice para la transmisión de la señal, el cual será factor determinante en las prestaciones (velocidad de transmisión y distancia) del sistema de comunicación. Íntimamente relacionado con las señales y los medios de transmisión está el problema de cómo codificar los datos en las señales a transmitir. Las técnicas de codificación son, igualmente, un factor que influirá en las prestaciones del sistema de transmisión.

Además de los tres conceptos fundamentales, a saber: la señal, el medio y la codificación, en la Parte II se estudian otros dos aspectos muy importantes en las comunicaciones de datos: la fiabilidad y la eficiencia. En cualquier esquema de comunicaciones, durante la transmisión, siempre habrá una tasa determinada de errores. Para el control del enlace de datos se necesitará un protocolo que proporcione los mecanismos para la detección y recuperación de los errores. Con ello, una línea que no sea fiable se convertirá en un enlace de datos fiable. Finalmente, si la capacidad del enlace es superior a lo requerido por una transmisión típica, en aras de proporcionar un uso eficaz del medio de transmisión, será necesario la utilización de varias técnicas de multiplexación.

ESQUEMA DE LA PARTE II

CAPÍTULO 3. TRANSMISIÓN DE DATOS

Los principios generales que rigen en la transmisión de datos están siempre subyacentes en todos los conceptos y técnicas que se presentan en este texto. Para comprender la necesidad de la codifi-

cación, la multiplexación, la conmutación, el control de errores, etc., el lector debería comprender previamente el comportamiento de la propagación de las señales a través de los medios de transmisión. En el Capítulo 3 se discuten las diferencias entre datos analógicos y digitales y entre la transmisión analógica y la digital. En este capítulo también se estudian los conceptos de atenuación y ruido.

CAPÍTULO 4. MEDIOS DE TRANSMISIÓN

Los medios de transmisión se pueden clasificar en guiados o inalámbricos. Los medios guiados más utilizados son el par trenzado, el cable coaxial y la fibra óptica. Entre las técnicas inalámbricas cabe destacar las microondas terrestres y vía satélite, la radiodifusión y los infrarrojos. En el Capítulo 4 se estudian todos estos conceptos.

CAPÍTULO 5. TÉCNICAS PARA LA CODIFICACIÓN DE SEÑALES

Los datos pueden ser analógicos (continuos) o digitales (discretos). Para su transmisión, se deben codificar mediante señales eléctricas de características acordes con el medio de transmisión. Tanto los datos analógicos como digitales se pueden representar mediante señales analógicas o digitales; cada una de las cuatro posibilidades se estudian en el Capítulo 5.

CAPÍTULO 6. TÉCNICAS DE COMUNICACIÓN DE DATOS DIGITALES

En el Capítulo 6, el interés se desplaza de la transmisión a la comunicación de datos. Para que dos dispositivos que están conectados mediante un medio de transmisión puedan intercambiar datos digitales se necesita un alto grado de cooperación entre ellos. Normalmente, los datos se transmiten de bit en bit. La temporización (la velocidad, la duración y la separación) de estos bits debe ser común en el transmisor y en el receptor. En este capítulo se exploran dos técnicas de comunicación habituales: la asíncrona y la síncrona. A continuación, se estudian los conceptos relacionados con los errores en la transmisión, la detección de errores y las técnicas de corrección. Generalmente, los dispositivos de datos digitales ni se conectan, ni transmiten directamente al medio. En su lugar, este proceso se lleva a cabo mediante la intervención de una interfaz normalizada.

CAPÍTULO 7. PROTOCOLOS DE CONTROL DEL ENLACE DE DATOS

El intercambio cooperativo de datos digitales entre dos dispositivos exige algún mecanismo para el control del enlace de datos. El Capítulo 7 estudia las técnicas fundamentales comunes a todos los protocolos para el control del enlace de datos, incluyendo el control del flujo y el control de los errores. A continuación, se estudia el protocolo más utilizado en esta capa: HDLC.

CAPÍTULO 8. MULTIPLEXACIÓN

Los equipos y servicios de transmisión son costosos. A menudo es habitual que dos estaciones interconectadas no utilicen toda la capacidad disponible del enlace de datos. Por cuestiones de rendimiento, sería deseable poder compartir esa capacidad. El término genérico con el que se denomina esa técnica es *multiplexación*.

El Capítulo 8 se centra en las tres técnicas más habituales de multiplexación. En primer lugar, se estudia la multiplexación más utilizada, la división en frecuencias (FDM, *Frecuency Division Multiplexing*), familiar para cualquiera que haya utilizado un receptor de radio o de televisión. La segunda técnica es un caso particular de multiplexación por división en el tiempo (TDM, *Time Division Multiplexing*) habitualmente denominada TDM síncrona. Esta técnica es habitual para la multiplexación de señales de voz digitalizada. El tercer tipo es otro caso particular de TDM, más compleja que la anterior pero potencialmente más eficaz, denominada TDM estadística o asíncrona.

CAPÍTULO 9. ESPECTRO EXPANDIDO

Las técnicas de espectro expandido se utilizan cada vez más en las comunicaciones inalámbricas. Dentro de ellas se consideran dos aproximaciones genéricas: el salto en frecuencias y el espectro expandido por secuencia directa. En el Capítulo 9 se proporciona un resumen de ambas técnicas. En este capítulo además se considera el concepto de acceso múltiple por división de código (CDMA, *Code Division Multiple Access*), que no es sino una aplicación del espectro expandido para proporcionar acceso múltiple a un canal compartido.

CAPÍTULO 3

Transmisión de datos

3.1. Conceptos y terminología
Terminología utilizada en transmisión de datos
Frecuencia, espectro y ancho de banda

3.2. Transmisión de datos analógicos y digitales
Datos analógicos y digitales
Señales analógicas y digitales
Transmisión analógica y digital

3.3. Dificultades en la transmisión
Atenuación
Distorsión de retardo
Ruido

3.4. Capacidad del canal
Ancho de banda de Nyquist
Fórmula para la capacidad de Shannon
El cociente E_b/N_0

3.5. Lecturas recomendadas

3.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

Apéndice 3A. Decibelios y energía de la señal

CUESTIONES BÁSICAS

- Todos los tipos de información considerados en este texto (voz, datos, imágenes, vídeo) se pueden representar mediante señales electromagnéticas. Para transportar la información, dependiendo del medio de transmisión y del entorno donde se realicen las comunicaciones, se podrán utilizar señales analógicas o digitales.

- Cualquier señal electromagnética, analógica o digital, está formada por una serie de frecuencias constituyentes. Un parámetro clave en la caracterización de la señal es el ancho de banda, definido como el rango de frecuencias contenidas en la señal. En términos generales, cuanto mayor es el ancho de banda de la señal, mayor es su capacidad de transportar información.

- Uno de los problemas principales en el diseño de un sistema de comunicaciones reside en paliar las dificultades, o defectos, de las líneas de transmisión. Las dificultades más importantes a superar son la atenuación, la distorsión de atenuación, la distorsión de retardo, así como los distintos tipos de ruido. El ruido puede ser, entre otros, de tipo térmico, ruido de intermodulación, diafonía o impulsivo. Al usar señales analógicas, las dificultades en la transmisión causan efectos de naturaleza aleatoria que degradan la calidad de la información recibida y pueden afectar a la inteligibilidad. Cuando se utilizan señales digitales, los defectos en la transmisión pueden introducir bits erróneos en la recepción.

- El diseñador de un sistema de comunicaciones debe tener presente cuatro factores determinantes: el ancho de banda de la señal, la velocidad de transmisión de la información digital, la cantidad de ruido, además de otros defectos en la transmisión, y, por último, la proporción o tasa de errores tolerable. El ancho de banda disponible está limitado por el medio de transmisión así como por la necesidad de evitar interferencias con señales cercanas. Debido a que el ancho de banda es un recurso escaso, es conveniente hacer máxima la velocidad de transmisión para el ancho de banda disponible. La velocidad de transmisión está limitada por el ancho de banda, por la presencia ineludible de defectos en la transmisión, como el ruido, y, finalmente, por la tasa de errores que sea tolerable.

El éxito en la transmisión de datos depende fundamentalmente de dos factores: la calidad de la señal que se transmite y las características del medio de transmisión. El objetivo de este capítulo, y del siguiente, es proporcionar al lector un conocimiento intuitivo de la naturaleza de estos dos factores.

La primera sección introduce algunos conceptos y terminología comúnmente aceptados en este campo, proporcionando así la base suficiente para abordar el resto del capítulo. La Sección 3.2 clarifica el uso de los conceptos *analógico* y *digital*. Tanto los datos analógicos como los digitales se pueden transmitir usando señales analógicas o digitales. Es más, esto es ampliable al procesamiento intermedio que se haga entre la fuente y el destino, pudiendo ser igualmente analógico o digital.

En la Sección 3.3 se estudian los defectos presentes en la transmisión que, en definitiva, pueden ser los causantes de los errores en los datos. Dichos errores son fundamentalmente: la atenuación, la distorsión en la atenuación, la distorsión de retardo y los diversos tipos de ruido existentes. Para concluir, se estudia el concepto fundamental de la capacidad del canal.

3.1. CONCEPTOS Y TERMINOLOGÍA

En esta sección se introducen algunos conceptos y términos que se utilizarán en este capítulo y, de hecho, a lo largo de toda la Parte II.

TERMINOLOGÍA UTILIZADA EN TRANSMISIÓN DE DATOS

La transmisión de datos entre un emisor y un receptor siempre se realiza a través de un medio de transmisión. Los medios de transmisión se pueden clasificar como guiados y no guiados. En ambos casos, la comunicación se realiza usando ondas electromagnéticas. En los **medios guiados**, por ejemplo en pares trenzados, en cables coaxiales y en fibras ópticas, las ondas se transmiten confinándolas a lo largo de un camino físico. Por el contrario, los medios **no guiados,** también denominados **inalámbricos,** proporcionan un medio para transmitir las ondas electromagnéticas sin confinarlas, como por ejemplo en la propagación a través del aire, el mar o el vacío.

El término **enlace directo** se usa para designar un camino de transmisión entre dos dispositivos en el que la señal se propague directamente del emisor al receptor sin ningún otro dispositivo intermedio que no sea un amplificador o repetidor. Estos últimos se usan para incrementar la energía de la señal. Obsérvese que este término se puede aplicar tanto a medios guiados como no guiados.

Un medio de transmisión guiado es **punto a punto** si proporciona un enlace directo entre dos dispositivos que comparten el medio, no existiendo ningún otro dispositivo conectado. En una configuración guiada **multipunto**, el mismo medio es compartido por más de dos dispositivos.

Un medio de transmisión puede ser *simplex*, *half-duplex* o *full-duplex*. En la transmisión ***simplex***, las señales se transmiten sólo en una única dirección; siendo una estación la emisora y otra la receptora. En ***half-duplex***, ambas estaciones pueden transmitir, pero no simultáneamente. En ***full-duplex***, ambas estaciones pueden igualmente transmitir y recibir, pero ahora simultáneamente. En este último caso, el medio transporta señales en ambos sentidos al mismo tiempo. Posteriormente se explicará cómo se realiza este tipo de transmisión. Nótese que estas definiciones son de uso común en los Estados Unidos (son definiciones ANSI). En otros lugares (donde prevalecen las definiciones UIT-T) el término *simplex* corresponde a *half-duplex*, tal y como se ha definido antes, y *duplex* se usa por lo que se ha definido como *full-duplex*.

FRECUENCIA, ESPECTRO Y ANCHO DE BANDA

En este texto, se estudiarán las señales electromagnéticas desde el punto de vista de la transmisión de datos. En el punto 3 de la Figura 1.2 se genera una señal en el transmisor que se enviará a través del medio. La señal, que es una función del tiempo, se puede expresar alternativamente en función de la frecuencia; es decir, la señal puede considerarse estar constituida por componentes a diferentes frecuencias. Para comprender y caracterizar el funcionamiento de los sistemas de transmisión de datos el **dominio de la frecuencia** suele ser más ilustrativo que el **dominio del tiempo**. A continuación, se introducen ambos dominios.

Conceptos en el dominio temporal

Toda señal electromagnética, considerada como función del tiempo, puede ser tanto analógica como digital. Una **señal analógica** es aquella en la que la intensidad de la señal varía suavemente en el tiempo. Es decir, no presenta saltos o discontinuidades[1].

[1] *N. del T.:* Por error en la edición 7.ª han dejado los títulos de la versión 6.ª. No obstante en la traducción se corrige.

Una **señal digital** es aquella en la que la intensidad se mantiene constante durante un determinado intervalo de tiempo, tras el cual la señal cambia a otro valor constante[2]. En la Figura 3.1 se muestran ejemplos de ambos tipos de señales. La señal continua puede corresponder a voz y la señal discreta puede representar valores binarios (0 y 1).

Las **señales periódicas** son el tipo de señales más sencillas que se puede considerar; se caracterizan por contener un patrón que se repite a lo largo del tiempo. En la Figura 3.2 se muestra un ejemplo de señal periódica continua (una onda sinusoidal) y un ejemplo de señal periódica discreta (una onda cuadrada). Matemáticamente, una señal $s(t)$ se dice periódica si y solamente si

$$s(t + T) = s(t) \qquad -\infty < t < +\infty$$

donde la constante T es el periodo de la señal (T debe ser el menor valor que verifique la ecuación). En cualquier otro caso la señal es **no periódica**.

La onda seno es una de las señales periódicas por antonomasia. Una onda seno genérica se representa mediante tres parámetros: la amplitud (A), la frecuencia (f) y la fase (ϕ). La **amplitud de pico** es el valor máximo de la señal en el tiempo; normalmente, este valor se mide en voltios. La **frecuencia** es la razón (en ciclos por segundo o Hercios (Hz)) a la que la señal se repite. Un parámetro equivalente es el **periodo** (T), definido como la cantidad de tiempo transcurrido entre dos repeticiones consecutivas de la señal; por tanto, se verifica que $T = 1/f$. La **fase** es una medida de la posición relativa de la señal dentro de un periodo de la misma; este concepto se explicará

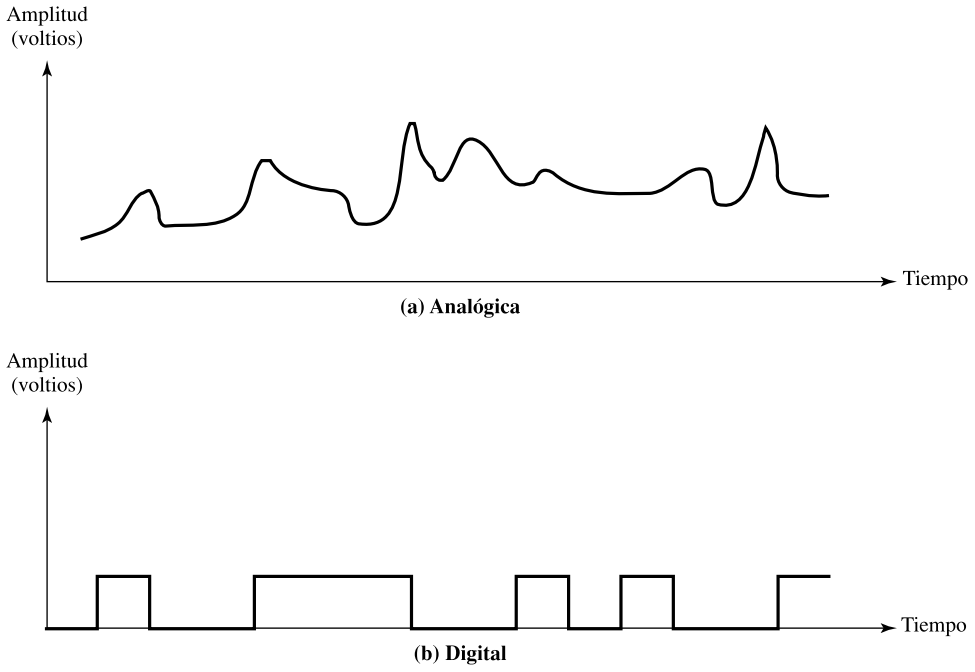
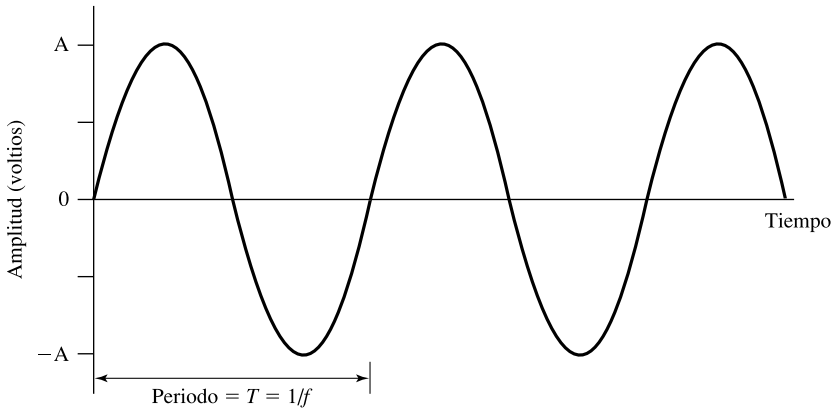
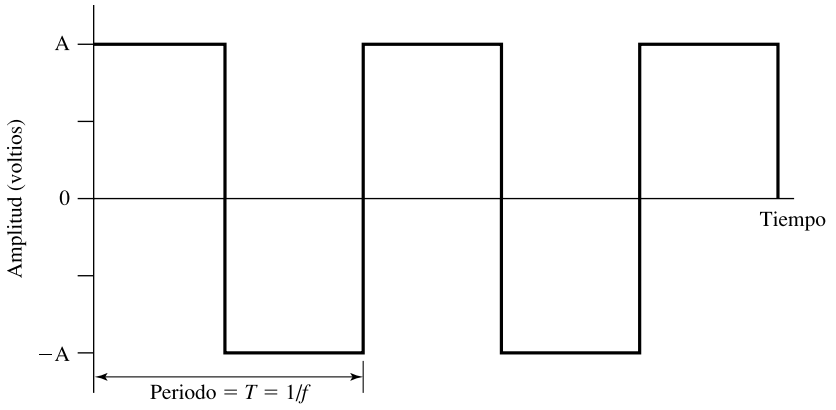


Figura 3.1. Señal analógica y señal digital.

[2] *N. del T.:* Por error en la edición 7.ª han dejado los títulos de la versión 6.ª. No obstante en la traducción se corrige.



(a) Onda sinusoidal



(b) Onda cuadrada

Figura 3.2. Ejemplos de señales periódicas.

más adelante. Más formalmente, en una señal periódica $f(t)$, la fase es la parte fraccionaria t/T del periodo T, en la que t ha avanzado respecto un origen arbitrario. El origen se considera normalmente como el último cruce por cero desde un valor negativo a uno positivo.

La expresión genérica para una onda sinusoidal es

$$s(t) = A \operatorname{sen}(2\pi f t + \phi)$$

En la Figura 3.3 se muestra el efecto de la variación de cada uno de los tres parámetros antes mencionados. En la parte (a) de la figura la frecuencia es 1 Hz, por tanto, el periodo $T = 1$ segundo. En la parte (b) se representa una onda seno con la misma fase y frecuencia pero con una amplitud de pico 0,5. En la parte (c) se tiene una señal con frecuencia $f = 2$, lo cual es equivalente a considerar un periodo $T = 0{,}5$. Por último, en la parte (d) de la misma figura se muestra el efecto de un desplazamiento en fase de $\pi/4$ radianes, que corresponde a 45 grados (2π radianes = 360^o = 1 periodo).

En la Figura 3.3, el tiempo se representa en el eje horizontal; la curva representa el valor de la señal en un punto del espacio dado en función del tiempo. Este tipo de gráficas, con un cambio

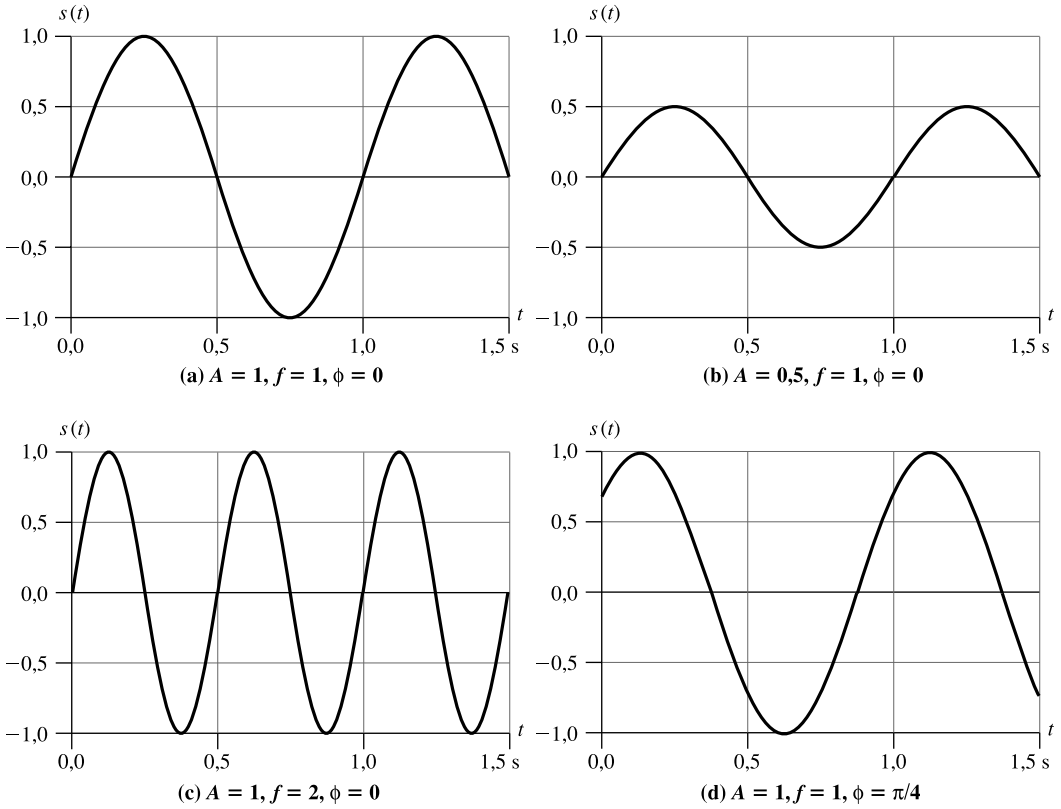


Figura 3.3. $s(t) = A\,\text{sen}\,(2\pi ft + \phi)$.

adicional de escala, también se usan representando la distancia en el eje horizontal. En este caso, la curva mostraría el valor de la señal para un instante de tiempo dado en función de la distancia. Por ejemplo, en una transmisión de una señal sinusoidal (léase una onda electromagnética de radiofrecuencia alejada a una cierta distancia de la antena, o un sonido alejado a cierta distancia del altavoz), en un instante determinado, la intensidad de la señal variará sinusoidalmente en función de la distancia desde la fuente.

Existe una relación sencilla entre las dos señales seno anteriores (en el tiempo y en el espacio). Dada una señal, se define la **longitud de onda,** λ, como la distancia que ocupa un ciclo o, en otras palabras, se define como la distancia entre dos puntos de igual fase en dos ciclos consecutivos. Supóngase que la señal se propaga a una velocidad v. En ese caso, la longitud de onda se puede relacionar con el periodo de la señal a través de la siguiente expresión: $\lambda = vT$, o de forma equivalente, $\lambda f = v$. Es de especial relevancia el caso en que $v = c$; es decir, cuando la velocidad de propagación en el medio es igual a la de la luz en el vacío, que como es sabido es aproximadamente 3×10^8 m/s.

Conceptos en el dominio de la frecuencia

En la práctica, las señales electromagnéticas pueden estar compuestas de muchas frecuencias. Por ejemplo, la señal

$$s(t) = (4/\pi) \times (\text{sen}\,(2\pi ft) + (1/3)\,\text{sen}\,(2\pi(3f)t))$$

se muestra en la Figura 3.4c. En este ejemplo la señal está compuesta por sólo dos términos seno correspondientes a las frecuencias f y $3f$; dichas componentes se muestran en las partes (a) y (b) de la mencionada figura. Hay dos comentarios interesantes que se pueden hacer a la vista de la figura:

- La frecuencia de la segunda componente es un múltiplo entero de la frecuencia de la primera. Cuando todas las componentes de una señal tienen frecuencias múltiplo de una dada, esta última se denomina **frecuencia fundamental**.

- El periodo de la señal total de componentes es el periodo correspondiente a la frecuencia fundamental. El periodo de la componente $(2\pi ft)$ es $T = 1/f$, y el periodo de $s(t)$ es también T, como se puede observar en la Figura 3.4c.

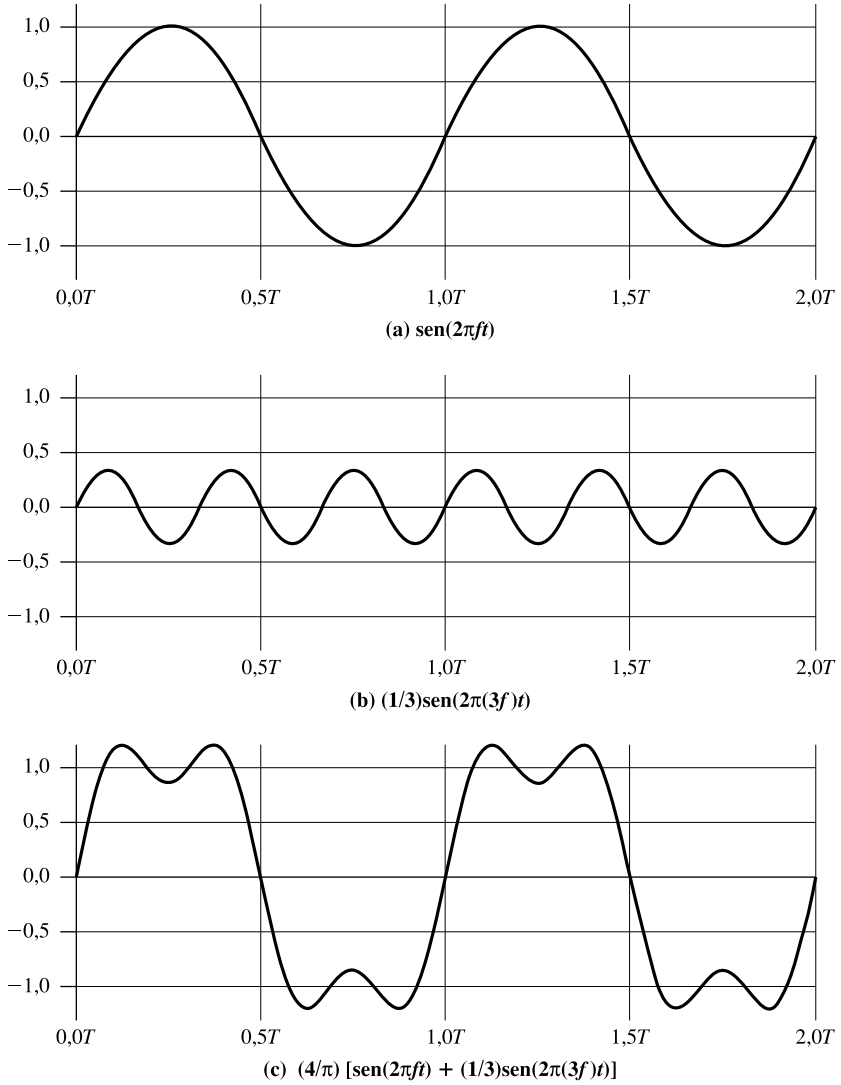


Figura 3.4. Suma de componentes en frecuencia ($T = 1/f$).

Se puede demostrar, usando el análisis de Fourier, que cualquier señal está constituida por componentes sinusoidales de distintas frecuencias. Sumando un número suficiente de señales sinusoidales, cada una con su correspondiente amplitud, frecuencia y fase, se puede construir cualquier señal electromagnética. En otras palabras, se puede demostrar cualquier señal electromagnética que está constituida por una colección de señales periódicas analógicas (ondas seno) con diferentes amplitudes, frecuencias y fases. La importancia de poder considerar una señal tanto en el dominio de la frecuencia, como en el dominio del tiempo se pondrá de manifiesto conforme vayamos avanzando en nuestro estudio. Para el lector interesado, en el Apéndice B se presenta una introducción al análisis de Fourier.

Por tanto, podemos decir que para cada señal hay una función en el dominio del tiempo $s(t)$ que determina la amplitud de la señal en cada instante del tiempo. Igualmente, hay una función $S(f)$, en el dominio de la frecuencia, que especifica las amplitudes de pico de las frecuencias constitutivas de la señal. En la Figura 3.5a se muestra la señal de la Figura 3.4c en el dominio de la

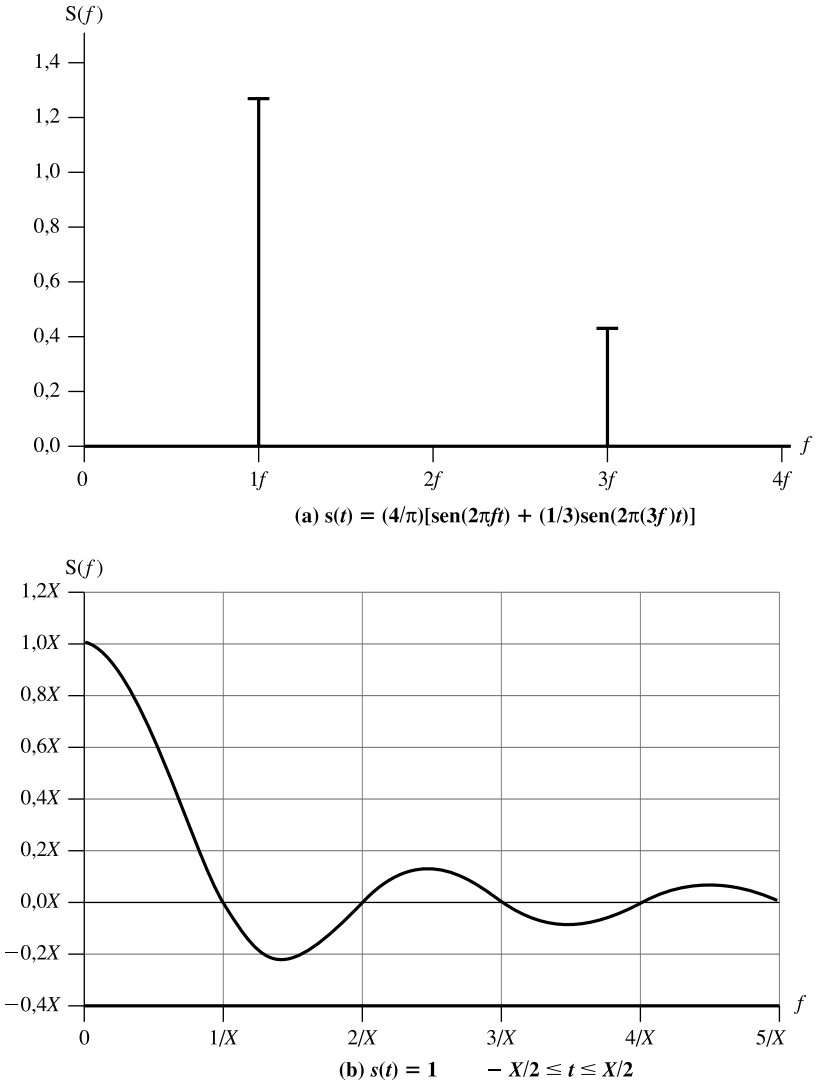


Figura 3.5. Representaciones en el dominio de la frecuencia.

frecuencia. Obsérvese que, en este caso, $S(f)$ es discreta. En la Figura 3.5b se muestra la función en el dominio de la frecuencia correspondiente a una señal pulso cuadrado, con valor 1 entre $-X/2$ y $X/2$, y 0 en cualquier otro caso[3]. Obsérvese que, en este caso, $S(f)$ es continua y tiene valores distintos de cero indefinidamente, aunque la magnitud de las componentes en frecuencias decrece rápidamente para frecuencias f grandes. Estos comportamientos son habituales en las señales reales.

Se define el **espectro** de una señal como el conjunto de frecuencias que la constituyen. Para la señal de la Figura 3.4c, el espectro se extiende desde f a $3f$. Se define el **ancho de banda absoluto** de una señal como la anchura del espectro. En el caso de la Figura 3.4c, el ancho de banda es $2f$. Muchas señales, como la de la Figura 3.5b, tienen un ancho de banda infinito. No obstante, la mayor parte de la energía de la señal se concentra en una banda de frecuencias relativamente estrecha. Esta banda se denomina **ancho de banda efectivo** o, simplemente, **ancho de banda**.

Para concluir, definiremos el término **componente continua** (**dc**). Si una señal contiene una componente de frecuencia cero, esa componente se denomina continua (dc, *direct current*). Por ejemplo, en la Figura 3.6 se muestra el resultado de sumarle una componente continua a la señal de la Figura 3.4c. Sin componente continua, la señal tiene una amplitud media igual a cero, vista en el

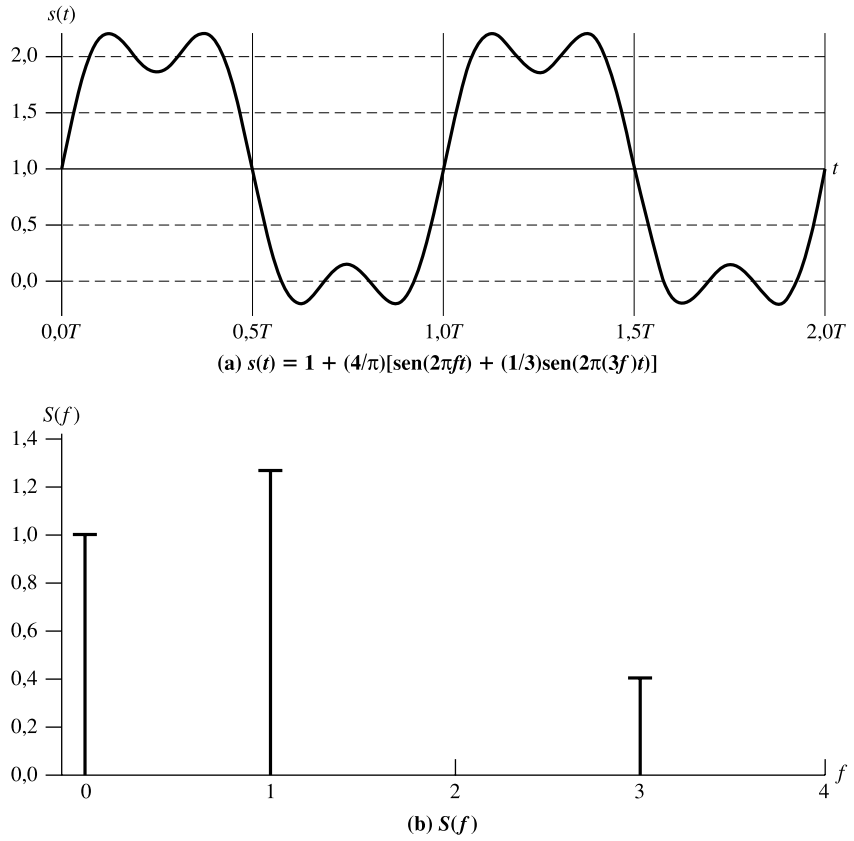


Figura 3.6. Señal con componente continua (dc).

[3] La definición matemática es: una señal $s(t)$ es continua si $\lim_{t \to a} s(t)$ para todo a.

dominio del tiempo. Si tiene componente continua, tendrá un término de frecuencia $f = 0$ y, por tanto, una amplitud promedio distinta de cero.

Relación entre la velocidad de transmisión y el ancho de banda

Se ha definido el ancho de banda efectivo como la banda en la que se concentra la mayor parte de la energía de la señal. *La mayor parte* es un concepto algo impreciso. La cuestión importante aquí es que, aunque una forma de onda dada contenga frecuencias en un rango extenso, por cuestiones prácticas, cualquier sistema de transmisión (transmisor más medio más receptor) sólo podrá transferir una banda limitada de frecuencias. Esto hace que la velocidad de transmisión máxima en el medio esté limitada.

Para explicar esta cuestión, consideremos la onda cuadrada de la Figura 3.2b. Supongamos que un 0 binario se representa mediante un pulso positivo y un 1 por un pulso negativo. Por tanto, la forma de onda representa la secuencia binaria 0101... La duración de cada pulso es $1/(2f)$; luego la velocidad de transmisión es $2f$ bits por segundo (bps). ¿Cuáles son las componentes en frecuencia de esta señal? Para responder a esta cuestión, consideremos de nuevo la Figura 3.4. Al sumar las ondas seno de frecuencias f y $3f$, se obtiene una forma de onda que empieza a parecerse a la onda cuadrada original. Continuemos el proceso sumando otra onda seno con frecuencia $5f$, como se muestra en la Figura 3.7a, y posteriormente sumando otra onda seno de frecuencia $7f$, también mostrada en la Figura 3.7b. Al sumar más términos múltiplos impares de la frecuencia f, convenientemente escalados, se irá aproximando la onda cuadrada cada vez con más precisión.

De hecho, se puede demostrar que las componentes en frecuencia de una onda cuadrada con amplitudes A y $-A$ se pueden expresar como

$$s(t) = A \times \frac{4}{\pi} \times \sum_{k \text{ impar}, k=1}^{\infty} \frac{\text{sen}\,(2\pi k f t)}{k}$$

Luego, esta forma de onda tiene un número infinito de componentes en frecuencia y, por tanto, un ancho de banda infinito. Sin embargo, la amplitud de pico de la componente k-ésima, kf, es solamente $1/k$. Por tanto, la mayor parte de la energía de esta forma de onda está contenida en las primeras componentes. ¿Qué ocurre si se limita el ancho de banda sólo a las tres primeras componentes? Ya hemos visto la respuesta en la Figura 3.7a. Como se puede ver, la forma de la onda resultante se aproxima razonablemente bien a la onda cuadrada original.

Las Figuras 3.4 y 3.7 pueden servir para ilustrar la relación entre la velocidad de transmisión y el ancho de banda. Supongamos que se está utilizando un sistema de transmisión digital capaz de transmitir señales con un ancho de banda de 4 MHz. Intentemos transmitir una secuencia de unos y ceros alternantes, como la onda cuadrada de la Figura 3.7c. ¿Qué velocidad de transmisión se puede conseguir? Para responder a esta pregunta consideremos los siguientes tres casos:

> **Caso I.** Aproximemos nuestra onda cuadrada con una forma de onda como la de la Figura 3.7a. Aunque es una forma de onda «distorsionada» es suficiente para que el receptor sea capaz de discriminar entre un 0 o un 1 binarios. Ahora bien, si tomamos una $f = 10^6$ ciclos/segundo = 1 MHz, entonces el ancho de banda de la señal
>
> $$s(t) = \frac{4}{\pi} \times \left[\text{sen}\,((2\pi \times 10^6)t) + \frac{1}{3}\text{sen}\,((2\pi \times 3 \times 10^6)t) + \frac{1}{5}\text{sen}\,((2\pi \times 5 \times 10^6)t) \right]$$

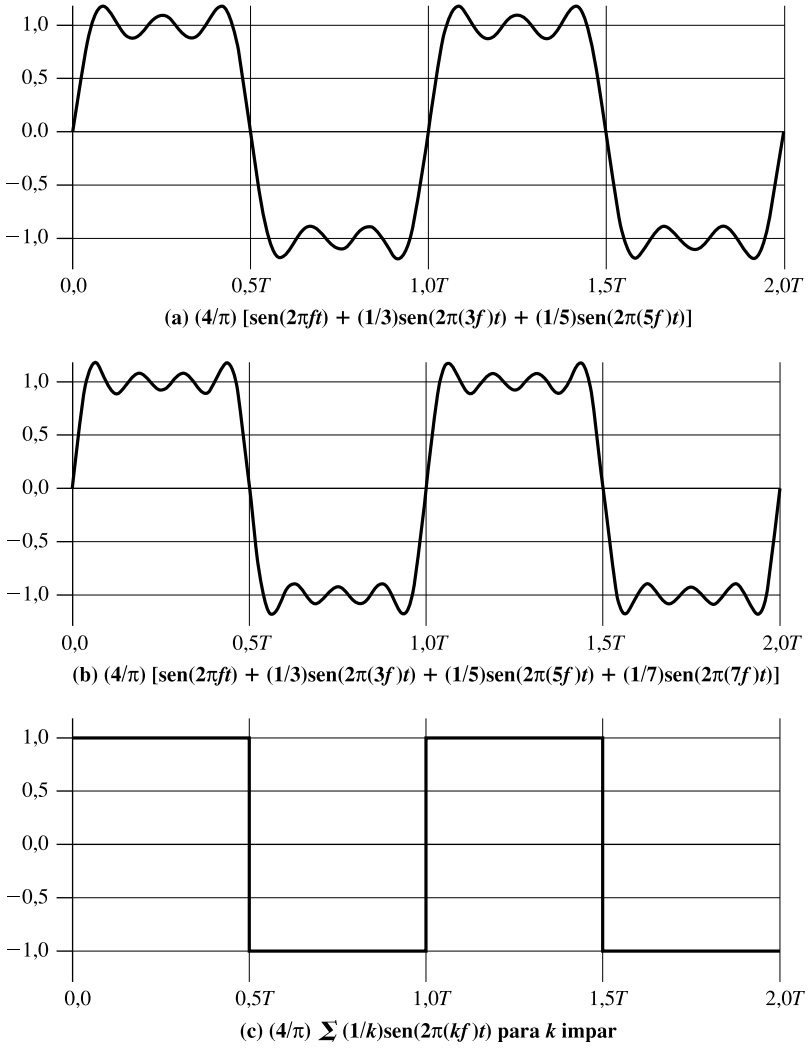


Figura 3.7. Componentes en frecuencia de una onda cuadrada ($T = 1/f$).

será igual a $(5 \times 10^6) - 10^6 = 4$ MHz. Obsérvese que para $f = 1$ MHz, el periodo de la frecuencia fundamental es $T = 1/10^6 = 10^{-6} = 1$ μs. Luego, si se considera esta forma de onda como una cadena de 0 y 1, un bit aparecerá cada 0,5 μs, lo que corresponde a una velocidad de $2 \times 10^6 = 2$ Mbps. Así, para un ancho de banda de 4 MHz, se consigue una velocidad de transmisión de 2 Mbps.

Caso II. Ahora supongamos que se dispone de un ancho de banda de 8 MHz. Considérese de nuevo la Figura 3.7a, pero ahora con $f = 2$ MHz. Usando un razonamiento idéntico al anterior, el ancho de banda de la señal es igual a $(5 \times 2 \times 10^6) - (2 \times 10^6) = 8$ MHz. Pero en este caso $T = 1/f = 0{,}5$ μs. Por tanto, aparece un bit cada 0,25 μs siendo la velocidad de transmisión, en este de caso, igual a 4 Mbps. Como conclusión, si se duplica el ancho de banda, dejando el resto de parámetros igual, se duplica la velocidad de transmisión potencial.

Caso III. Ahora supongamos que la forma de onda de la Figura 3.4c se considera adecuada para aproximar una onda cuadrada. Es decir, la diferencia entre un pulso positivo y un pulso negativo en la Figura 3.4c es suficientemente grande para que la forma de onda pueda representar adecuadamente la secuencia de unos y ceros. Supóngase, como en el caso II, que $f = 2$ MHz y que $T = 1/f = 0{,}5$ μs, de tal manera que aparece un bit cada 0,25 μs, siendo la velocidad de transmisión igual a 4 Mbps. Considerando la Figura 3.4c, el ancho de banda de la señal es igual a $(3 \times 2 \times 10^6) - (2 \times 10^6) = 4$ MHz. Por tanto, un ancho de banda dado puede proporcionar varias velocidades de transmisión, dependiendo de la habilidad que exhiba el receptor para distinguir diferencias entre los 1 y 0 en presencia de ruido y de otros defectos.

Resumiendo,

- **Caso I:** ancho de banda = 4 MHz, velocidad de transmisión = 2 Mbps.
- **Caso II:** ancho de banda = 8 MHz, velocidad de transmisión = 4 Mbps.
- **Caso III:** ancho de banda = 4 MHz, velocidad de transmisión = 4 Mbps.

De las observaciones precedentes, se pueden extraer las siguientes conclusiones. En general, cualquier onda digital tendrá un ancho de banda infinito. Si se intenta transmitir esta forma de onda como una señal por cualquier medio, el sistema de transmisión limitará el ancho de banda que se puede transmitir. Es más, para cualquier medio, cuanto mayor sea el ancho de banda transmitido, mayor será el coste. Luego, por un lado, razones prácticas y económicas sugieren que la información digital se aproxime por una señal de ancho de banda limitado. Por otro lado, limitar el ancho de banda introduce distorsiones, las cuales hacen que la interpretación de la señal recibida sea más difícil. Cuanto mayor es la limitación en el ancho de banda, mayor es la distorsión y mayor es la posibilidad de que se cometan errores en el receptor.

Una ilustración adicional puede servir para reforzar estos conceptos. En la Figura 3.8 se muestra una cadena de bits con una velocidad de transmisión de 2.000 bits por segundo. Con un ancho de banda igual a 2.500 Hz, o incluso 1.700 Hz, la representación es bastante buena. Es más, estos resultados son generalizables de la siguiente manera. Si la velocidad de transmisión de la señal digital es W bps, entonces se puede obtener una representación muy buena con un ancho de banda de $2W$ Hz. No obstante, a menos que el ruido sea muy elevado, la secuencia de bits se puede recuperar con un ancho de banda menor (*véase* el apartado dedicado a la capacidad del canal en la Sección 3.4).

Por tanto, hay una relación directa entre la velocidad de transmisión y el ancho de banda: cuanto mayor es la velocidad de transmisión de la señal, mayor es el ancho de banda efectivo necesitado. Visto de otra manera, cuanto mayor es el ancho de banda de un sistema de transmisión, mayor es la velocidad con la que se pueden transmitir los datos en el sistema.

Otra observación interesante es la siguiente: si consideramos que el ancho de banda de una señal está centrado sobre una frecuencia dada, denominada **frecuencia central**, cuanto mayor sea dicha frecuencia central, mayor es el ancho de banda potencial y, por tanto, mayor puede ser la velocidad de transmisión. Por ejemplo, para una señal centrada en torno a 2 MHz, su ancho de banda máximo es de 4 MHz.

Posteriormente, tras el estudio de las dificultades presentes en la transmisión, en la Sección 3.4 se volverá a la discusión de la relación entre el ancho de banda y la velocidad de transmisión.

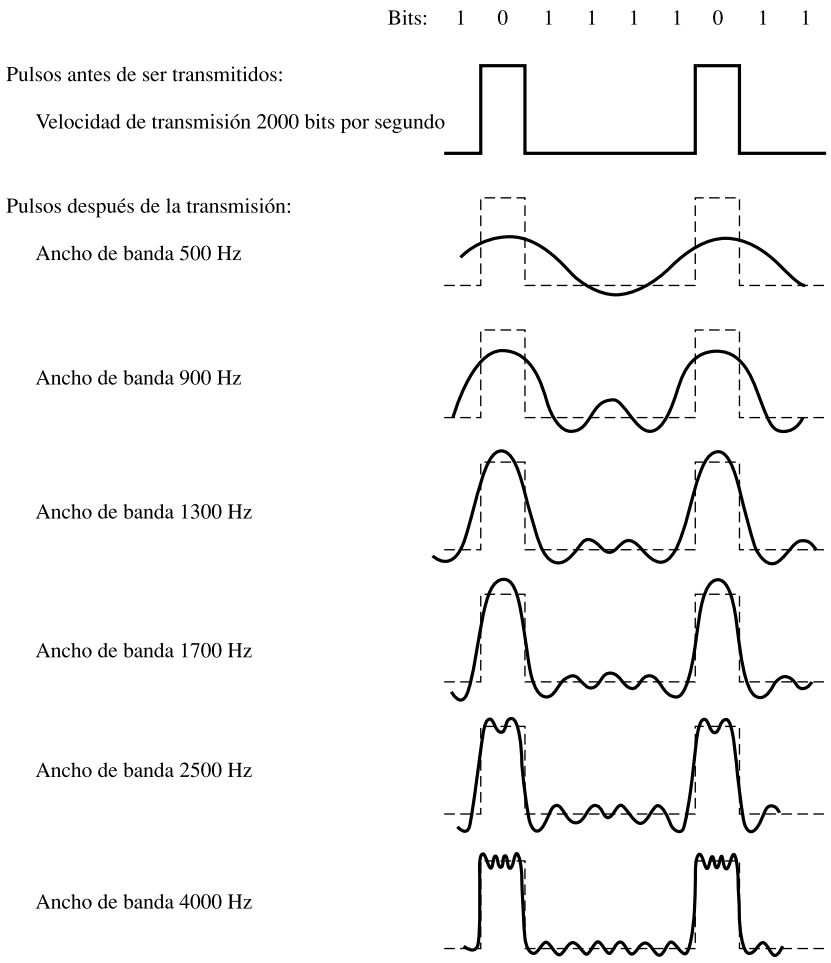

Bits: 1 0 1 1 1 1 0 1 1
Pulsos antes de ser transmitidos:
Velocidad de transmisión 2000 bits por segundo
Pulsos después de la transmisión:
Ancho de banda 500 Hz
Ancho de banda 900 Hz
Ancho de banda 1300 Hz
Ancho de banda 1700 Hz
Ancho de banda 2500 Hz
Ancho de banda 4000 Hz

Figura 3.8. Efecto del ancho de banda en las señales digitales.

3.2. TRANSMISIÓN DE DATOS ANALÓGICOS Y DIGITALES

Los términos *analógico* y *digital* corresponden respectivamente, por lo general, a *continuo* y *discreto*. Estos dos términos se aplican con frecuencia en el marco de las comunicaciones en al menos tres contextos diferentes: datos, señalización y transmisión.

Escuetamente, se define **dato** como cualquier entidad capaz de transportar información. Las **señales** son representaciones eléctricas o electromagnéticas de los datos. La **señalización** es el hecho de la propagación física de las señales a través de un medio adecuado. Por último, se define **transmisión** como la comunicación de datos mediante la propagación y el procesamiento de señales. En lo que sigue, se intentará clarificar estos conceptos abstractos, considerando las diferencias entre los términos *analógico* y *digital* referidos a los datos, las señales y la transmisión.

DATOS ANALÓGICOS Y DIGITALES

Los conceptos de datos analógicos o digitales son bastante sencillos. Los datos analógicos pueden tomar valores en un intervalo continuo. Por ejemplo, el vídeo y la voz son valores de intensidad

que varían continuamente. La mayor parte de los datos que se capturan con sensores, como los de temperatura y de presión, toman valores continuos. Los datos digitales toman valores discretos, como por ejemplo las cadenas de texto o los números enteros.

El ejemplo más familiar o cercano de datos analógicos es la señal de **audio**, la cual se puede percibir directamente por los seres humanos en forma de ondas de sonido. La Figura 3.9 muestra el espectro acústico de la voz humana y de las señales de música[4]. Se pueden encontrar componentes en frecuencia entre 100 Hz y 7 kHz. Aunque la mayor parte de la energía de la voz está concentrada en las frecuencias bajas, experimentalmente se ha demostrado que las frecuencias por debajo de 600 o 700 Hz contribuyen poco a la inteligibilidad de la voz en el oído humano. Una señal de voz típica tiene un rango dinámico aproximadamente de 25 dB[5], es decir, la potencia máxima es del orden de 300 veces superior a la potencia mínima. La Figura 3.9 también muestra el espectro y rango dinámico de la señal de música.

Otro ejemplo típico de datos analógicos es el **vídeo**. En este caso, es más fácil caracterizar los datos en términos del espectador (o destino) de la pantalla de TV, que en términos de la escena original (o fuente) que se graba en la cámara de TV. Para producir una imagen en la pantalla, un haz de electrones barre la superficie de la pantalla de izquierda a derecha y de arriba a abajo. En la televisión en blanco y negro la iluminación (en una escala del negro al blanco) que se produce en un punto determinado es proporcional a la intensidad del haz cuando pasa por ese punto. Por tanto, en cualquier instante de tiempo el haz toma un valor de intensidad analógico para así producir el brillo deseado en ese punto de la pantalla. Es más, cuando el haz hace el barrido, el valor analógico cambia. Por tanto, la imagen de vídeo se puede considerar como una señal analógica variable en el tiempo.

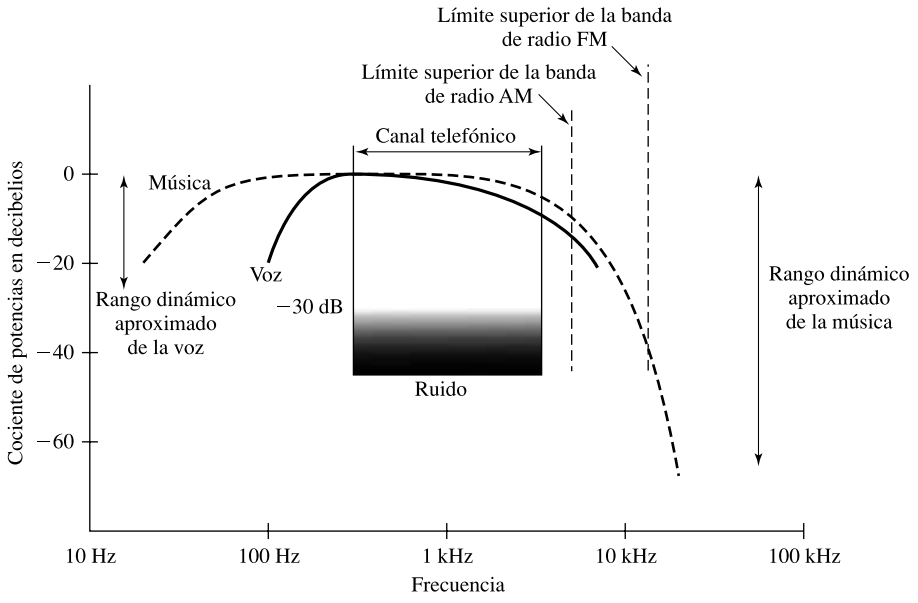


Figura 3.9. Espectro acústico de la voz y música [CARN99a].

[4] Ésta es una definición ideal. De hecho, la transición entre un nivel de tensión y otro no puede ser instantánea, ya que siempre habrá un pequeño periodo de transición. No obstante, una señal digital real se aproxima mucho al modelo ideal de niveles constantes de tensión con transiciones instantáneas.

[5] De hecho, la función $S(f)$ en este ejemplo es simétrica respecto $f = 0$ y, por tanto, está definida para valores negativos de la frecuencia. La existencia de frecuencias negativas es un artificio matemático cuya justificación cae fuera del propósito de este texto.

La Figura 3.10a muestra el proceso de barrido. Al final de cada línea de barrido, el haz se vuelve rápidamente hacia la izquierda (retroceso horizontal). Cuando el haz alcanza la parte más baja, se vuelve rápidamente a la línea superior (retroceso vertical). Obsérvese que el haz se anula durante los retrocesos.

Para conseguir una resolución adecuada, el haz describe un total de 483 líneas horizontales a una velocidad de 30 barridos de pantalla por segundo. Después de diversas pruebas se ha demostrado que esa velocidad produciría una sensación de parpadeo, en lugar de una sensación de movimiento suave, como sería deseable. Para producir una imagen sin parpadeo, y sin incrementar con ello el ancho de banda requerido, se utiliza una técnica denominada **entrelazado**. Tal y como se muestra en la Figura 3.10b, las líneas pares e impares se escanean por separado de forma alternante en los campos par e impar respectivamente. El campo impar corresponde al escaneado desde A hasta B y el campo par desde C hasta D. El haz alcanza la mitad de la línea inferior de la pantalla tras barrer 214,5 líneas. En ese instante, el haz se reposiciona rápidamente a lo alto de la pantalla, volviendo a la mitad de la línea superior de la pantalla visible, para generar las 241,5 líneas adicionales entrelazadas con las originales. Así pues, la pantalla se refresca 60 veces por segundo, en lugar de las 30 anteriores, y con ello se elimina el parpadeo.

Las cadenas de caracteres, o de **texto,** son un ejemplo típico de datos digitales. Mientras que los datos en formato de texto son más adecuados para los seres humanos, en general, no se pueden

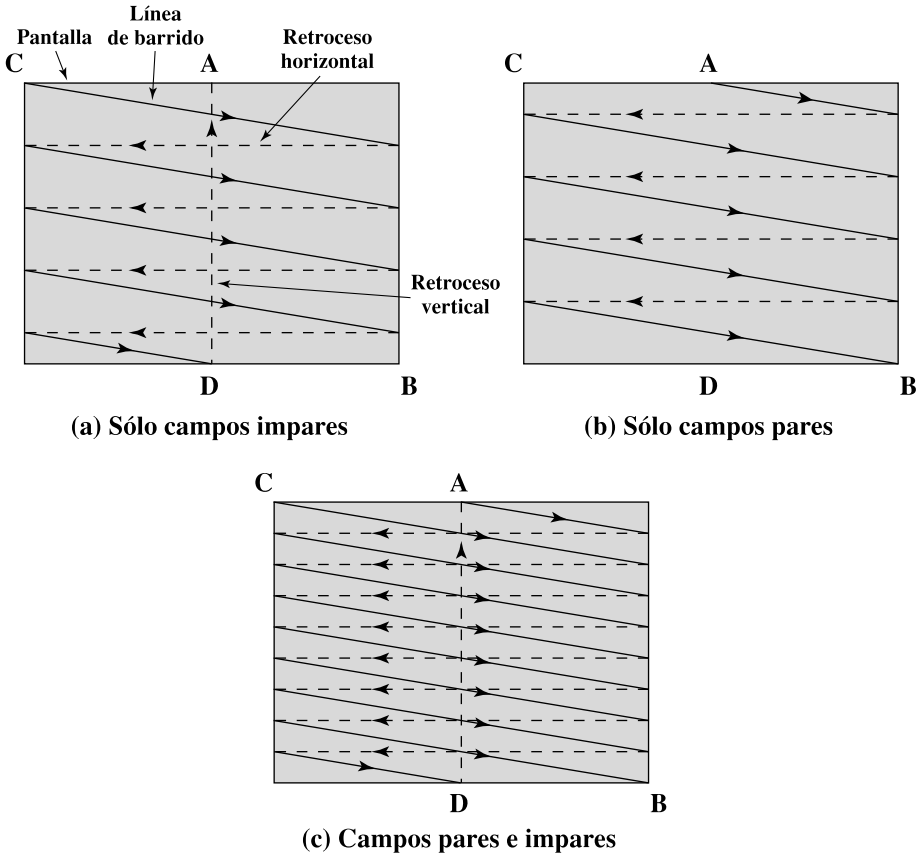


Figura 3.10. Barrido de vídeo entrelazado.

transmitir o almacenar fácilmente (en forma de caracteres) en los sistemas de procesamiento o comunicación. Tales sistemas están diseñados para tratar datos binarios. Para esto se han diseñado un gran número de códigos mediante los cuales los caracteres se representan como secuencias de bits. Quizá, el ejemplo más antiguo y conocido es el código Morse. En nuestros días, el código más utilizado es el Alfabeto de Referencia Internacional (IRA, *International Reference Alphabet*)[6]. Cada carácter se representa en este código por un patrón único de 7 bits; por tanto, se pueden representar 128 caracteres distintos. Esto implica un número mayor del necesario, por lo que algunos patrones, de entre los 128, se utilizan como *caracteres de control*. Los caracteres codificados con IRA se almacenan o transmiten casi siempre usando 8 bits por carácter. El bit número 8 se utiliza como bit de paridad para la detección de errores. Este bit se elige de forma tal que el número de unos binarios en el octeto sea siempre impar (paridad impar) o siempre par (paridad par). Así pues, se podrán detectar los errores de transmisión que cambien un único bit o cualquier número impar de ellos.

SEÑALES ANALÓGICAS Y DIGITALES

En un sistema de comunicaciones, los datos se propagan de un punto a otro mediante señales electromagnéticas. Una señal analógica es una onda electromagnética que varía continuamente y que, según sea su espectro, puede propagarse a través de una serie de medios; por ejemplo, a través de un medio guiado como un par trenzado, un cable coaxial, un cable de fibra óptica, o a través de medios no guiados, como la atmósfera o el espacio. Una señal digital es una secuencia de pulsos de tensión que se puede transmitir a través de un medio conductor; por ejemplo, un nivel de tensión positiva constante puede representar un 0 binario y un nivel de tensión negativa constante puede representar un 1.

La principal ventaja de la señalización digital es que en términos generales, es más económica que la analógica, a la vez de ser menos susceptible a las interferencias de ruido. La principal desventaja es que las señales digitales sufren más con la atenuación que las señales analógicas. En la Figura 3.11 se muestra una secuencia de pulsos de tensión, generados por una fuente que utiliza dos niveles. También se muestra la tensión recibida en algún punto distante de un medio conductor. Debido a la atenuación, o reducción, de la energía de la señal que sufren las frecuencias altas, los pulsos se hacen más pequeños a la vez que se suavizan. Esta atenuación puede implicar perder con facilidad la información contenida en la señal propagada.

A continuación, se darán algunos ejemplos específicos de tipos de señales y, posteriormente, se discutirán las relaciones existentes entre datos y señales.

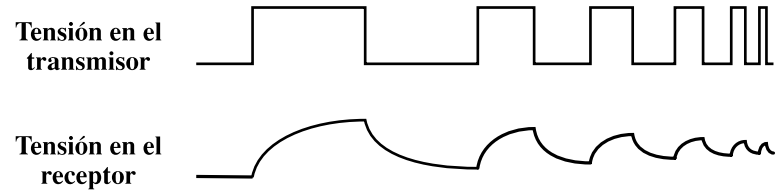


Figura 3.11. Atenuación de señales digitales.

[6] Nótese que en el eje *x* se usa una escala logarítmica. De igual forma, como el eje *y* está en decibelios, en realidad es escala logarítmica también. En el documento de repaso de matemáticas del sitio web de recursos para estudiantes de computación, localizado en WilliamStallings.com/StudentsSupport.html, hay un resumen sobre las escalas logarítmicas.

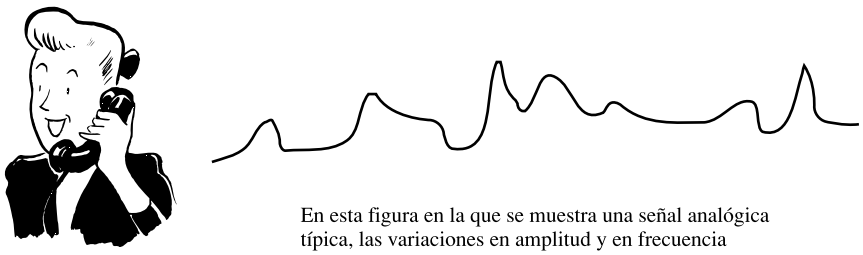
Ejemplos

Volvamos a los tres ejemplos de la sección anterior. Para cada uno de ellos, se describirá la señal y su ancho de banda estimado.

El ejemplo más típico de información analógica es el audio, o información acústica, la cual se percibe directamente por los seres humanos como ondas de sonido. Un tipo de información acústica es, desde luego, la voz humana, la cual tiene componentes en frecuencias desde los 20 Hz a los 20 kHz. Para su transmisión, este tipo de información se puede convertir fácilmente a una señal electromagnética (*véase* Figura 3.12). En particular, todas las frecuencias sonoras, cuya amplitud se mide en términos de sonoridad, se convierten a frecuencias electromagnéticas, cuyas amplitudes se miden en voltios. Los teléfonos tienen un mecanismo sencillo para realizar esta conversión.

En el caso de datos acústicos (voz), los datos se pueden representar directamente mediante una señal electromagnética que ocupe el mismo espectro. Sin embargo, es necesario establecer un compromiso entre la fidelidad del sonido cuando se vaya a transmitir eléctricamente y el coste de la transmisión, el cual aumentará al aumentar el ancho de banda. Aunque, como ya se ha mencionado, el espectro de la voz está aproximadamente entre 100 Hz y 7 kHz, un ancho de banda mucho más estrecho producirá una calidad aceptable. El espectro estándar para las señales de voz está entre 300 y 3.400 Hz. Esta reducción es adecuada para la transmisión de la voz, ya que a la vez se reduce la capacidad de transmisión necesaria y se posibilita el uso de teléfonos de coste muy bajo. Así pues, el teléfono transmisor convierte la señal acústica de entrada en una señal electromagnética en el rango de 300 a 3.400 Hz. Esta señal se transmite a través del sistema telefónico al receptor, el cual la reproduce generando un sonido acústico.

Ahora consideremos la señal de vídeo. Para generar la señal de vídeo se usa una cámara de TV, que en realidad realiza funciones similares a un receptor de TV. Un componente de la cámara es una placa fotosensible, sobre la que se enfoca ópticamente la imagen. Un haz de electrones barre la placa de izquierda a derecha y de arriba abajo, de igual manera que en la Figura 3.10. Al efectuar el barrido, se genera una señal eléctrica proporcional a la intensidad de la imagen en cada punto particular. Como ya se ha mencionado, se barren 483 líneas a una razón de 30 barridos completos por segundo. Estos números son aproximados, ya que se pierde tiempo en el retroceso vertical del haz de barrido. El estándar en EE.UU. es de 525 líneas, de las cuales se pierden 42 durante el retroceso vertical. Por tanto, la frecuencia de barrido horizontal es (525 líneas) × (30 barridos/s) = 15.750 líneas por segundo, o lo que es lo mismo 63,5 μs/línea. De estos 63,5 μs/línea, aproximadamente 11 μs están reservados para el retroceso horizontal, quedando pues un total de 52,5 μs por línea de vídeo.



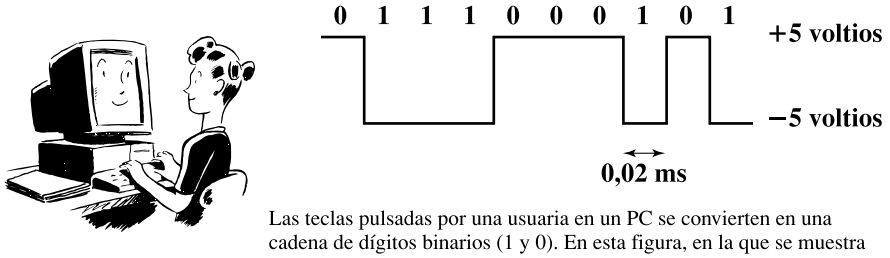
En esta figura en la que se muestra una señal analógica típica, las variaciones en amplitud y en frecuencia transportan la evolución temporal de la sonoridad y la frecuencia fundamental de la voz o de la música. Para transmitir TV, se usan señales similares, pero con frecuencias mucho más altas.

Figura 3.12. Conversión de voz a señal analógica.

Estamos ya en disposición de estimar el ancho de banda que se necesita para la señal de vídeo. Para hacer esto se deben estimar las frecuencias superior (máxima) e inferior (mínima) de la banda. Utilizaremos el siguiente razonamiento para determinar la frecuencia máxima: dicha frecuencia ocurriría durante el barrido horizontal si la imagen cambiara alternativamente de blanco a negro tan rápido como fuera posible. Se puede estimar el valor máximo considerando la resolución de la imagen de vídeo. En la dimensión vertical hay 483 líneas, de forma tal que la resolución vertical máxima sería 483. Experimentalmente se ha demostrado que la resolución real subjetiva es alrededor del 70% de ese número, es decir, 338 líneas. Para conseguir una imagen compensada, las resoluciones vertical y horizontal deberán ser aproximadamente las mismas. La resolución horizontal debería ser $4/3 \times 338 = 450$ líneas, ya que la relación de la anchura de la pantalla de TV respecto a la altura es de 4:3. En el peor de los casos, la línea de barrido consistiría en 450 elementos alternantes de blanco y negro. El barrido resultante sería una onda en la que cada ciclo consistiría en dos niveles de tensión correspondientes al negro (el mayor) y al blanco (el inferior). Por tanto, habría $450/2 = 225$ ciclos de la onda cada 52,5 μs, proporcionando una frecuencia máxima de 4,2 MHz. Este razonamiento aproximado es, en realidad, bastante preciso. El límite inferior será una frecuencia cero o continua, donde el valor de continua corresponde a la iluminación promedio de la imagen (es decir, el valor promedio en el que la señal supera el nivel de referencia del negro). Por tanto, el ancho de banda de la señal de vídeo es aproximadamente 4 MHz − 0 = 4 MHz.

En la discusión anterior no se han considerado ni las componentes de color ni las de audio. Obsérvese que si se incluyen dichas componentes el ancho de banda sigue siendo aproximadamente 4 MHz.

Finalmente, el tercer ejemplo mencionado anteriormente es el correspondiente a datos binarios digitales. La información binaria se genera en terminales, computadores y otros equipos para el procesamiento de datos; posteriormente, para su transmisión, se convierte a pulsos digitales de tensión, como se muestra en la Figura 3.13. Normalmente, para estos datos se usan dos niveles de tensión constante (dc), un nivel para el 1 binario y otro para el 0 (en el Capítulo 5, se verá que ésta es una de las posibles alternativas, llamada NRZ). Lo interesante aquí es el ancho de banda de dicha señal. Éste dependerá de la forma de la onda exacta y de la secuencia de unos y ceros. Para una mejor comprensión, considérese la Figura 3.8 y compárese con la Figura 3.7. Como se puede observar, al aumentar el ancho de banda de la señal, la aproximación a la cadena de pulsos digitales es mejor.



Las teclas pulsadas por una usuaria en un PC se convierten en una cadena de dígitos binarios (1 y 0). En esta figura, en la que se muestra una señal digital típica, el 1 binario se representa con −5 voltios y el 0 binario se representa con +5 voltios. El elemento de señal para cada bit tiene una duración de 0,02 ms, lo que implica una velocidad de transmisión igual a 50.000 bits por segundo (50 kbps).

Figura 3.13. Conversión de la entrada de un PC a señal digital.

Datos y señales

En la discusión anterior se han considerado señales analógicas para representar datos analógicos y señales digitales para representar datos digitales. Generalmente, los datos analógicos son función del tiempo y ocupan un espectro en frecuencias limitado; estos datos se pueden representar mediante una señal electromagnética que ocupe el mismo espectro. Los datos digitales se pueden representar mediante señales digitales con un nivel de tensión diferente para cada uno de los dígitos binarios.

Como se muestra en la Figura 3.14, éstas no son las únicas posibilidades. Los datos digitales se pueden también representar mediante señales analógicas usando un *módem* (modulador/demodulador). El módem convierte la serie de pulsos binarios de tensión (bi-valuados) en una señal analógica, codificando los datos digitales haciendo variar alguno de los parámetros característicos de una señal denominada *portadora*. La señal resultante ocupa un cierto espectro de frecuencias centrado

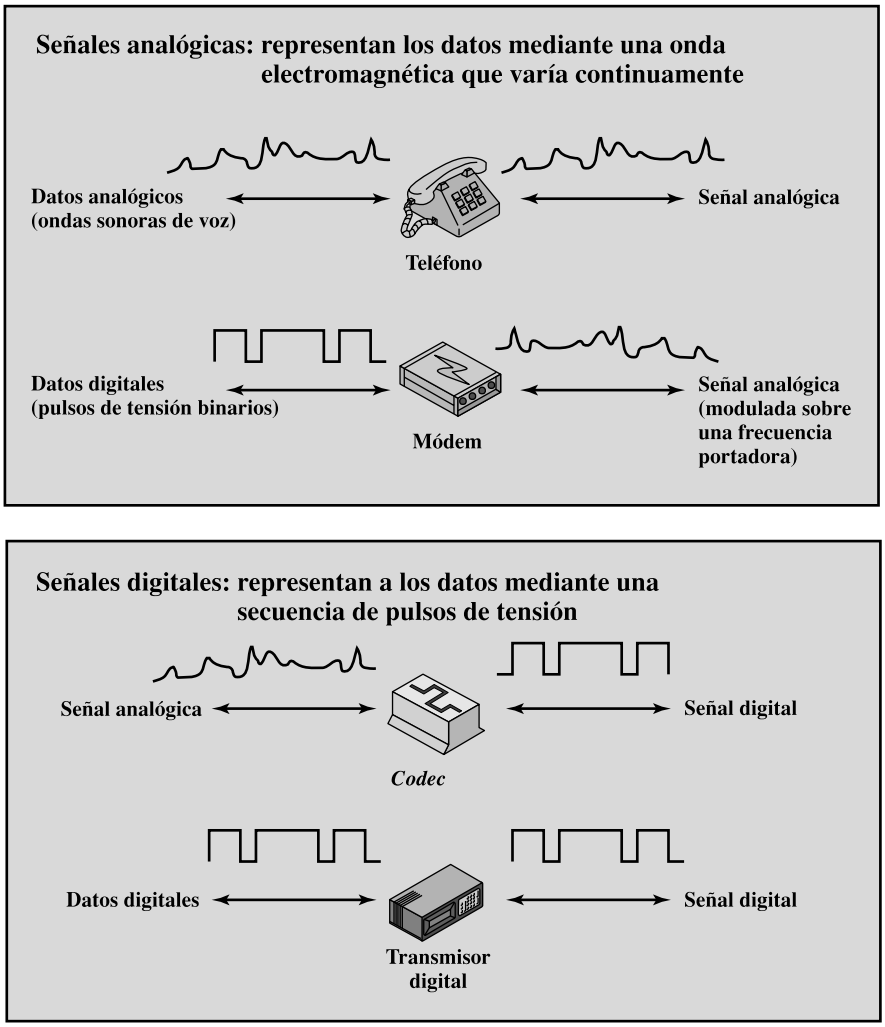

Señales analógicas: representan los datos mediante una onda electromagnética que varía continuamente
Datos analógicos (ondas sonoras de voz)
Señal analógica
Teléfono
Datos digitales (pulsos de tensión binarios)
Señal analógica (modulada sobre una frecuencia portadora)
Módem
Señales digitales: representan a los datos mediante una secuencia de pulsos de tensión
Señal analógica
Señal digital
Codec
Datos digitales
Señal digital
Transmisor digital

Figura 3.14. Señalización analógica y digital de datos analógicos y digitales.

en torno a la frecuencia de la portadora. De esta manera se podrán transmitir datos digitales a través de medios adecuados a la naturaleza de la señal portadora. Los módem más convencionales representan los datos binarios en el espectro de la voz y, por tanto, hacen posible que los datos se propaguen a través de líneas telefónicas convencionales. En el otro extremo de la línea, el módem demodula la señal para recuperar los datos originales.

Realizando una operación muy similar a la que realizan los módem, los datos analógicos se pueden representar mediante señales digitales. El dispositivo que realiza esta función para la voz se denomina *codec* (codificador-decodificador). Esencialmente, el *codec* toma la señal analógica, que representa directamente a la voz, y la aproxima mediante una cadena de bits. En el receptor, dichos bits se usan para reconstruir los datos analógicos.

Así pues, la Figura 3.14 sugiere que los datos se pueden codificar de varias maneras. Este punto se volverá a tratar en el Capítulo 5.

TRANSMISIÓN ANALÓGICA Y DIGITAL

Tanto las señales analógicas como las digitales se pueden transmitir si se emplea el medio de transmisión adecuado. El medio de transmisión en concreto determinará cómo se tratan estas señales. En la Tabla 3.1 se resumen los métodos de transmisión de datos. La **transmisión analógica** es una forma de transmitir señales analógicas con independencia de su contenido; las señales pueden representar datos analógicos (por ejemplo, voz) o datos digitales (por ejemplo, los datos binarios modulados en un módem). En cualquier caso, la señal analógica se irá debilitando (atenuándose) con la distancia. Para conseguir distancias más largas, el sistema de transmisión analógico incluye amplificadores que inyectan energía en la señal. Desgraciadamente, el amplificador también inyecta energía en las componentes de ruido. Para conseguir distancias mayores, al utilizar amplificadores en cascada, la señal se distorsiona cada vez más. En el caso de los datos analógicos, como la voz, se puede tolerar una pequeña distorsión, ya que en ese caso los datos siguen siendo inteligibles. Sin embargo, para los datos digitales los amplificadores en cascada introducirán errores.

La **transmisión digital**, por el contrario, es dependiente del contenido de la señal. Una señal digital sólo se puede transmitir a una distancia limitada, ya que la atenuación, el ruido y otros aspectos negativos pueden afectar a la integridad de los datos transmitidos. Para conseguir distancias mayores se usan repetidores. Un repetidor recibe la señal digital, regenera el patrón de ceros y unos, y los retransmite. De esta manera se evita la atenuación.

Para señales analógicas se puede usar la misma técnica anterior si la señal transmitida transporta datos digitales. En este caso, el sistema de transmisión tendrá repetidores convenientemente espaciados en lugar de amplificadores. Dichos repetidores recuperan los datos digitales a partir de la señal analógica y generan una señal analógica limpia. De esta manera, el ruido no es acumulativo.

Un problema a resolver es la elección del mejor método de transmisión. Para resolver este problema, la industria de las telecomunicaciones y sus usuarios han optado por la transmisión digital. Tanto las comunicaciones a larga distancia, como los servicios de comunicación a distancias cortas (por ejemplo, entre edificios) se han reconvertido a digital y, lo que es más, la señalización digital se está introduciendo en todos los sistemas donde sea factible. Las razones más importantes que justifican esta elección son:

- **Tecnología digital:** las mejoras en las tecnologías de integración a gran escala (LSI) y a muy gran escala (VLSI) se han traducido en una disminución continua, tanto en coste como en el tamaño, de la circuitería digital. Los equipos analógicos no han experimentado una reducción similar.

Tabla 3.1. Transmisión analógica y digital.

(a) Datos y señales

	Señal analógica	Señal digital
Datos analógicos	Hay dos alternativas (1) la señal ocupa el mismo espectro que los datos analógicos; (2) los datos analógicos se codifican ocupando una porción distinta del espectro.	Los datos analógicos se codifican utilizando un *codec* para generar una cadena de bits.
Datos digitales	Los datos digitales se codifican usando un módem para generar señal analógica.	Hay dos alternativas (1) la señal consiste en dos niveles de tensión que representan dos valores binarios (2) los datos digitales se codifican para producir una señal digital con las propiedades deseadas.

(b) Tratamiento de señales

	Transmisión analógica	Transmisión digital
Señal analógica	Se propaga a través de amplificadores; se trata de igual manera si la señal se usa para representar datos analógicos o digitales.	Se supone que la señal analógica representa datos digitales. La señal se propaga a través de repetidores; en cada repetidor, los datos digitales se obtienen de la señal de entrada y se usan para regenerar una nueva señal analógica de salida.
Señal digital	No se usa.	La señal digital representa una cadena de unos o ceros, los cuales pueden representar datos digitales o pueden ser resultado de la codificación de datos analógicos. La señal se propaga a través de repetidores; en cada repetidor, se recupera la cadena de unos y ceros a partir de la señal de entrada, a partir de los cuales se genera la nueva cadena de salida.

- **Integridad de los datos:** al usar repetidores en lugar de amplificadores, el ruido y otros efectos negativos no son acumulativos. Por tanto, usando tecnología digital es posible transmitir datos conservando su integridad a distancias mayores utilizando incluso líneas de calidad inferior.

- **Utilización de la capacidad:** en términos económicos, el tendido de líneas de transmisión de banda ancha ha llegado a ser factible, incluso para medios como canales vía satélite y fibra óptica. Para usar eficazmente todo ese ancho de banda se necesita un alto grado de mutiplexación. La multiplexación se puede realizar más fácilmente y con menor coste usando técnicas digitales (división en el tiempo) que con técnicas analógicas (división en frecuencia). Estas cuestiones se estudiarán en el Capítulo 8.

- **Seguridad y privacidad:** las técnicas de cifrado se pueden aplicar fácilmente a los datos digitales o a los analógicos que se hayan digitalizado previamente.

- **Integración:** en el tratamiento digital de datos analógicos y digitales todas las señales tienen igual forma y pueden ser procesadas de una forma similar. Este hecho posibilita economías de gran escala mediante la integración de voz, vídeo y datos.

3.3. DIFICULTADES EN LA TRANSMISIÓN

En cualquier sistema de comunicaciones se debe aceptar que la señal que se recibe diferirá de la señal transmitida debido a varias adversidades y dificultades sufridas en la transmisión. En las señales analógicas, estas dificultades pueden degradar la calidad de la señal. En las señales digitales, se generarán bits erróneos: un 1 binario se transformará en un 0 y viceversa. En este apartado se van a estudiar las dificultades mencionadas comentando sus efectos sobre la capacidad de transportar información en los enlaces de transmisión; en el Capítulo 5 se presentan algunas medidas a tomar para paliar el efecto de estas dificultades.

Las dificultades más significativas son:

- La atenuación y la distorsión de atenuación.
- La distorsión de retardo.
- El ruido.

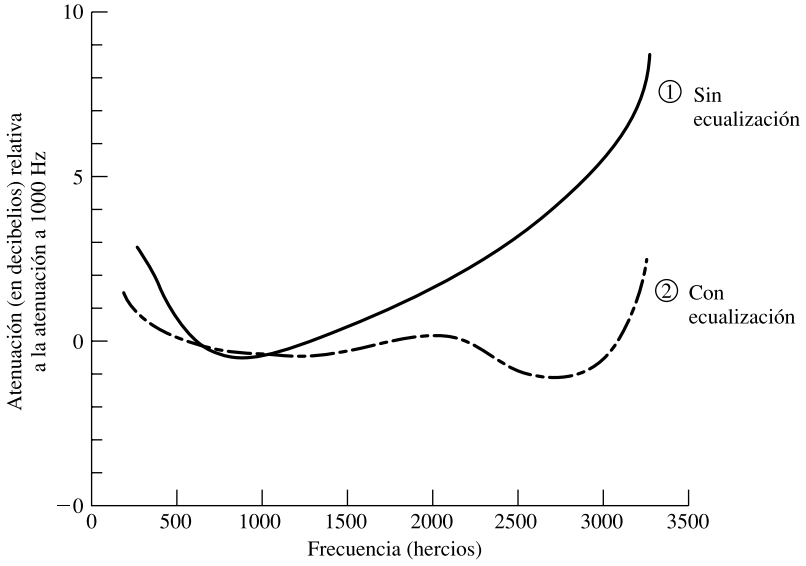
ATENUACIÓN

En cualquier medio de transmisión la energía de la señal decae con la distancia. En medios guiados, esta reducción de la energía es por lo general exponencial y, por tanto, se expresa generalmente como un número constante en decibelios por unidad de longitud. En medios no guiados, la atenuación es una función más compleja de la distancia y es dependiente, a su vez, de las condiciones atmosféricas. Se pueden establecer tres consideraciones respecto a la atenuación. Primera, la señal recibida debe tener suficiente energía para que la circuitería electrónica en el receptor pueda detectar la señal adecuadamente. Segunda, para ser recibida sin error, la señal debe conservar un nivel suficientemente mayor que el ruido. Tercera, la atenuación es habitualmente una función creciente de la frecuencia.

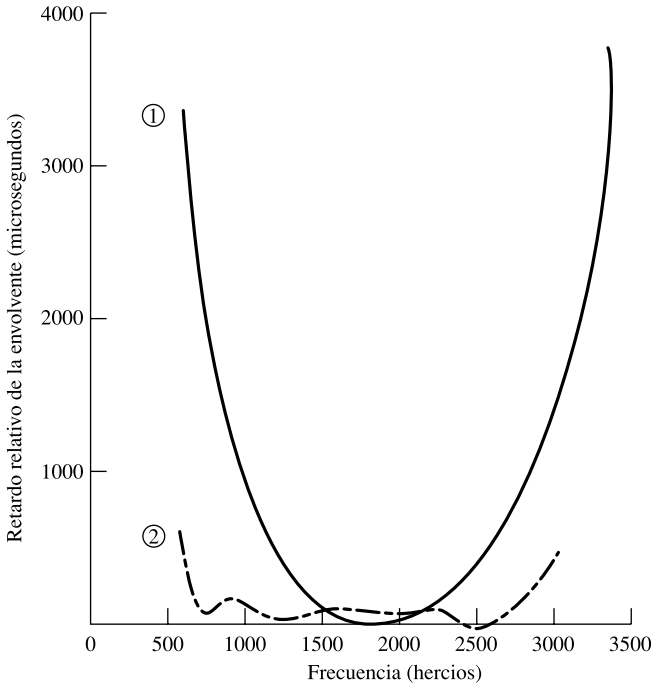
Los dos primeros problemas se resuelven controlando la energía de la señal, para ello se usan amplificadores o repetidores. En un enlace punto a punto, la energía de la señal en el transmisor debe ser lo suficientemente elevada como para que se reciba con inteligibilidad, pero no tan elevada que sature la circuitería del transmisor o del receptor, lo que generaría una señal distorsionada. A partir de cierta distancia, la atenuación es inaceptable, lo que requiere la utilización de repetidores o amplificadores que realcen la señal periódicamente. Este tipo de problemas son todavía más complejos en líneas multipunto, en las que la distancia entre el transmisor y el receptor es variable.

El tercer problema es especialmente relevante para el caso de las señales analógicas. Debido a que la atenuación varía en función de la frecuencia, la señal recibida está distorsionada, reduciendo así la inteligibilidad. Para soslayar este problema, existen técnicas para ecualizar la atenuación en una banda de frecuencias dada. En las líneas telefónicas esto se realiza cambiando las propiedades eléctricas de la línea, usando normalmente bobinas de carga, las cuales suavizan los efectos de la atenuación. Otra aproximación alternativa es la utilización de amplificadores que amplifiquen más las frecuencias altas que las bajas.

En la Figura 3.15a se incluye un ejemplo, en el que se representa la atenuación como función de la frecuencia para una línea convencional. En dicha figura, la atenuación se ha obtenido como una medida relativa respecto de la atenuación a 1.000 Hz. Los valores positivos en el eje *y* representan atenuaciones mayores que la sufrida a 1.000 Hz. A la entrada se aplica un tono a 1.000 Hz



(a) Atenuación



(b) Distorsión de retardo

Figura 3.15. Distorsión de atenuación y de retardo para un canal de voz.

con una potencia conocida, posteriormente se mide la potencia $P_{1.000}$ en la salida. Este procedimiento se repite para cualquier otra frecuencia f, y la atenuación relativa en decibelios es[7]

$$N_f = -100 \log_{10} \frac{P_f}{P_{1.000}}$$

En la Figura 3.15a la línea continua muestra la atenuación sin ecualización. Como se puede observar, las componentes en frecuencia en el extremo superior de la banda de voz se atenúan mucho más que las componentes en bajas frecuencias. Es evidente que esto distorsiona la señal de voz recibida. La línea discontinua muestra los efectos de la ecualización. Al aplanar la atenuación relativa, se consigue una mejora en la calidad de la señal de voz. Esto también permite, al usar un módem para transmitir datos digitales, una velocidad superior.

La distorsión de atenuación es un problema mucho menor para las señales digitales. Como ya se ha mencionado, la energía de la señal digital decae rápidamente con la frecuencia (*véase* Figura 3.5b); la mayor parte de sus componentes están concentradas en torno a la frecuencia fundamental o velocidad de transmisión (en bits/segundo o bps) de la señal.

DISTORSIÓN DE RETARDO

La distorsión de retardo es un fenómeno debido a que la velocidad de propagación de una señal a través de un medio guiado varía con la frecuencia. Para una señal limitada en banda, la velocidad tiende a ser mayor cerca de la frecuencia central y disminuye al acercarse a los extremos de la banda. Por tanto, las distintas componentes en frecuencia de la señal llegarán al receptor en instantes diferentes de tiempo, dando lugar a desplazamientos de fase entre las diferentes frecuencias.

Este efecto se llama distorsión de retardo, ya que la señal recibida está distorsionada debido al retardo variable que sufren sus componentes. La distorsión de retardo es particularmente crítica en la transmisión de datos digitales. Supóngase que se está transmitiendo una secuencia de bits, utilizando una señal analógica o digital. Debido a la distorsión de retardo, algunas de las componentes de la señal en un bit se desplazarán hacia otras posiciones, provocando interferencia entre símbolos. Este hecho es un factor (de gran importancia) que limita la velocidad de transmisión máxima en un canal de transmisión.

Para compensar la distorsión de retardo también se pueden emplear técnicas de ecualización. Usando de nuevo como ejemplo una línea telefónica, en la Figura 3.15b se muestra el efecto de la ecualización del retardo en función de la frecuencia.

RUIDO

Para cualquier dato transmitido, la señal recibida consistirá en la señal transmitida modificada por las distorsiones introducidas en la transmisión, además de señales no deseadas que se insertarán en algún punto entre el emisor y el receptor. A estas últimas señales no deseadas se les denomina ruido. El ruido es el factor de mayor importancia de entre los que limitan las prestaciones de un sistema de comunicación.

[7] El concepto de decibelio se explica en el Apéndice 3A.

La señal de ruido se puede clasificar en cuatro categorías:

- Ruido térmico.
- Ruido de intermodulación.
- Diafonía.
- Ruido impulsivo.

El **ruido térmico** se debe a la agitación térmica de los electrones. Está presente en todos los dispositivos electrónicos y medios de transmisión; como su nombre indica, es función de la temperatura. El ruido térmico está uniformemente distribuido en el espectro de frecuencias usado en los sistemas de comunicación, es por esto por lo que a veces se denomina ruido blanco. El ruido térmico no se puede eliminar y, por tanto, impone un límite superior en las prestaciones de los sistemas de comunicación. Es especialmente dañino en las comunicaciones satelitales ya que, en estos sistemas, la señal recibida por las estaciones terrestres es muy débil. En cualquier dispositivo o conductor, la cantidad de ruido térmico presente en un ancho de banda de 1 Hz es

$$N_0 = kT\,(\mathrm{W/Hz})$$

donde[8]

N_0 = densidad de potencia del ruido, en vatios por 1 Hz de ancho de banda.

k = constante de Boltzmann = $1{,}38 \times 10^{-23}$ J/K.

T = temperatura absoluta, en grados Kelvin.

Ejemplo 3.1. A temperatura ambiente, es decir a $T = 17\,^{\circ}\mathrm{C}$, o 290 K, la densidad de potencia del ruido térmico será:

$$N_0 = (1{,}38 \times 10^{-23}) \times 290 = 4 \times 10^{-21}\ \mathrm{W/Hz} = -204\ \mathrm{dBW/Hz}$$

donde dBW corresponde a decibelios-vatio, unidad definida en el Apéndice 3A.

Se supone que el ruido es independiente de la frecuencia. Así pues, el ruido térmico presente en un ancho de banda de B hercios se puede expresar como

$$N = kTB$$

o, expresado en decibelios-vatio,

$$\begin{aligned} N &= 10\log k + 10\log T + 10\log B \\ &= -228{,}6\ \mathrm{dBW} + 10\log T + 10\log B \end{aligned}$$

[8] IRA se define en la Recomendación de la UIT-T T.50. Inicialmente se denominó *International Alphabet Number* 5 (IA5). La versión del IRA en EE.UU. se denomina *American Standard Code for Information Interchange* (ASCII). En la página web del libro se puede encontrar una descripción y una tabla con el código IRA.

Ejemplo 3.2. Dado un receptor con una temperatura efectiva de ruido de 294 K y un ancho de banda de 10 MHz, el ruido térmico a la salida del receptor será

$$\begin{aligned} N &= -228{,}6 \text{ dBW} + 10/\log(294) + 10\log 10^7 \\ &= -228{,}6 + 24{,}7 + 70 \\ &= -133{,}9 \text{ dBW} \end{aligned}$$

Cuando señales de distintas frecuencias comparten el mismo medio de transmisión puede producirse **ruido de intermodulación**. El efecto del ruido de intermodulación es la aparición de señales a frecuencias que sean suma o diferencia de las dos frecuencias originales o múltiplos de éstas. Por ejemplo, la mezcla de las señales de frecuencias f_1 y f_2 puede producir energía a frecuencia $f_1 + f_2$. Estas componentes espúreas podrían interferir con otras componentes a frecuencia $f_1 + f_2$.

El ruido de intermodulación se produce cuando hay alguna no linealidad en el transmisor, en el receptor o en el sistema de transmisión. Idealmente, estos sistemas se comportan como sistemas lineales; es decir, la salida es igual a la entrada multiplicada por una constante. Sin embargo, en cualquier sistema real, la salida es una función más compleja de la entrada. El comportamiento no lineal puede aparecer debido al funcionamiento incorrecto de los sistemas o por sobrecargas producidas al utilizar señales con mucha energía. Bajo estas circunstancias es cuando aparecen los términos suma o diferencia no deseados.

La **diafonía** la ha podido experimentar todo aquel que al usar un teléfono haya oído otra conversación; se trata, en realidad, de un acoplamiento no deseado entre las líneas que transportan las señales. Esto puede ocurrir por el acoplamiento eléctrico entre cables de pares cercanos o, en raras ocasiones, en líneas de cable coaxial que transporten varias señales. La diafonía también puede aparecer cuando las señales no deseadas se captan en las antenas de microondas; aunque éstas se caracterizan por ser altamente direccionales, la energía de las microondas se dispersa durante la transmisión. Generalmente, la diafonía es del mismo orden de magnitud (o inferior) que el ruido térmico.

Los ruidos antes descritos son de magnitud constante y razonablemente predecibles. Así pues, es posible idear un sistema de transmisión que les haga frente. Por el contrario, el **ruido impulsivo** es no continuo y está constituido por pulsos o picos irregulares de corta duración y de amplitud relativamente grande. Se generan por una gran diversidad de causas, por ejemplo, por perturbaciones electromagnéticas exteriores producidas por tormentas atmosféricas o por fallos y defectos en los sistemas de comunicación.

Generalmente, el ruido impulsivo no tiene mucha transcendencia para los datos analógicos. Por ejemplo, la transmisión de voz se puede perturbar mediante chasquidos o crujidos cortos, sin que ello implique pérdida significativa de inteligibilidad. Sin embargo, el ruido impulsivo es una de las fuentes principales de error en la comunicación digital de datos. Por ejemplo, un pico de energía con duración de 0,01 s no inutilizaría datos de voz, pero podría corromper aproximadamente 560 bits si se transmitieran a 56 kbps. La Figura 3.16 muestra un ejemplo del efecto del ruido sobre una señal digital. Aquí el ruido consiste en un nivel relativamente pequeño de ruido térmico más picos ocasionales de ruido impulsivo. Los datos digitales se recuperan muestreando la señal recibida una vez por cada intervalo de duración del bit. Como se puede observar, el ruido es a veces suficiente para convertir un 1 en un 0, o un 0 en un 1.

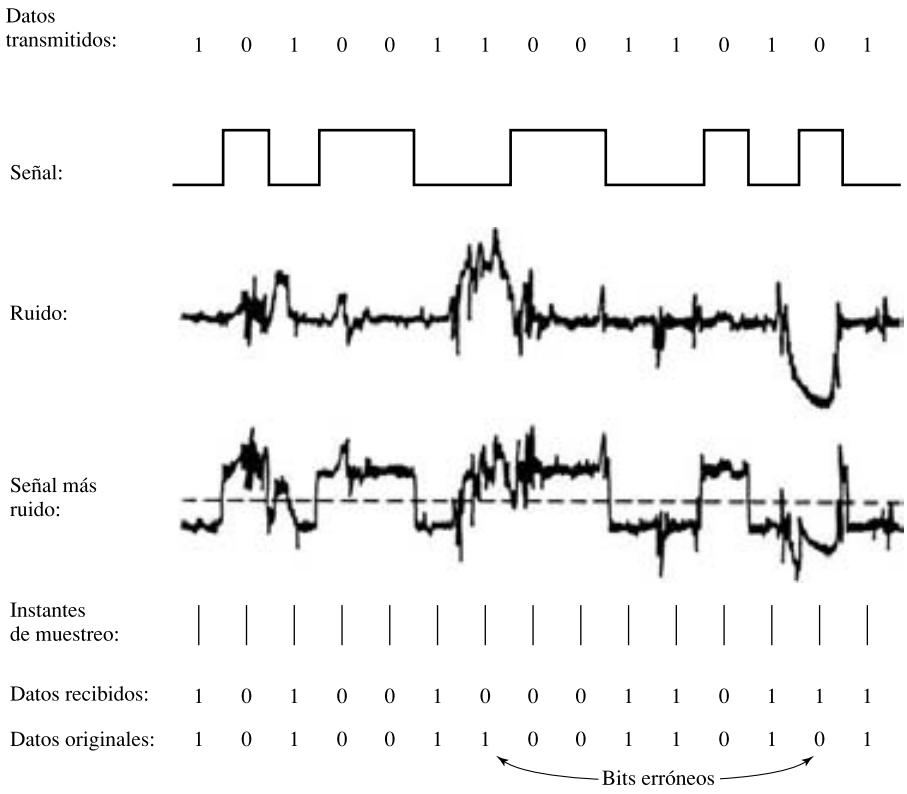

Datos transmitidos:
1 0 1 0 0 1 1 0 0 1 1 0 1 0 1
Señal:
Ruido:
Señal más ruido:
Instantes de muestreo:
Datos recibidos: 1 0 1 0 0 1 0 0 0 1 1 0 1 1 1
Datos originales: 1 0 1 0 0 1 1 0 0 1 1 0 1 0 1
Bits erróneos

Figura 3.16. Efecto del ruido en una señal digital.

3.4. CAPACIDAD DEL CANAL

Previamente se ha estudiado que hay una gran variedad de efectos nocivos que distorsionan o corrompen la señal. Para los datos digitales, la cuestión a resolver es en qué medida estos defectos limitan la velocidad con la que se pueden transmitir. Se denomina **capacidad del canal** a la velocidad máxima a la que se pueden transmitir los datos en un canal, o ruta de comunicación de datos, bajo unas condiciones dadas.

Hay cuatro conceptos en juego relacionados entre sí, que son:

- **La velocidad de transmisión de los datos:** velocidad, expresada en bits por segundo (bps), a la que se pueden transmitir los datos.
- **El ancho de banda:** ancho de banda de la señal transmitida; éste estará limitado por el transmisor y por la naturaleza del medio de transmisión; se mide en ciclos por segundo o hercios.
- **El ruido:** nivel medio de ruido a través del camino de transmisión.
- **La tasa de errores:** tasa a la que ocurren los errores. Se considera que ha habido un error cuando se recibe un 1 habiendo transmitido un 0, o se recibe un 0 habiendo transmitido un 1.

El problema considerado aquí es el siguiente: los servicios de comunicaciones son por lo general caros y, normalmente, cuanto mayor es el ancho de banda requerido por el servicio, mayor es el coste. Es más, todos los canales de transmisión de interés práctico están limitados en banda. Las limitaciones surgen de las propiedades físicas de los medios de transmisión o por limitaciones que se imponen deliberadamente en el transmisor para prevenir interferencias con otras fuentes. Por consiguiente, es deseable hacer un uso tan eficiente como sea posible del ancho de banda limitado. En el caso de los datos digitales, esto significa que dado un ancho de banda sería deseable conseguir la mayor velocidad de datos posible no superando la tasa de errores permitida. El mayor inconveniente para conseguir este objetivo es la existencia de ruido.

ANCHO DE BANDA DE NYQUIST

Para comenzar, considérese el caso de un canal exento de ruido. En este entorno, la limitación en la velocidad de los datos está impuesta simplemente por el ancho de banda de la señal. Nyquist formalizó esta limitación, afirmando que si la velocidad de transmisión de la señal es $2B$, entonces una señal con frecuencias no superiores a B es suficiente para transportar esta velocidad de transmisión de la señal. Y viceversa: dado un ancho de banda B, la mayor velocidad de transmisión de la señal que se puede conseguir es $2B$. Esta limitación está provocada por la interferencia entre símbolos que se produce por la distorsión de retardo. Este resultado es de utilidad en el diseño de convertidores digital a analógico; en la página web del libro se facilita su demostración.

Obsérvese que en el último párrafo nos hemos referido a la velocidad de la señal. Si las señales a transmitir son binarias (dos niveles de tensión), la velocidad de transmisión de datos que se puede conseguir con B Hz es igual a $2B$ bps. Por ejemplo, considérese un canal de voz que se utiliza mediante un módem para transmitir datos digitales. Supóngase un ancho de banda de 3100 Hz. Entonces, la capacidad C del canal es $2B = 6.200$ bps. No obstante, como se verá en el Capítulo 5, se pueden usar señales con más de dos niveles; es decir, cada elemento de señal puede representar a más de dos bits. Por ejemplo, si se usa una señal con cuatro niveles de tensión, cada elemento de dicha señal podrá representar dos bits. La formulación de Nyquist para el caso de señales multinivel es

$$C = 2B \log_2 M$$

donde M es el número de señales discretas o niveles de tensión. Así pues, para $M = 8$, valor típico que se usa en algunos módem, la capacidad resulta ser 18.600 bps, siendo el ancho de banda igual a 3.100 Hz.

Por tanto, para un ancho de banda dado, la velocidad de transmisión de datos se puede incrementar considerando un número mayor de señales diferentes. Sin embargo, esto supone una dificultad mayor en el receptor: en lugar de tener que distinguir una de entre dos señales, deberá distinguir una de entre M posibles señales. El ruido y otras dificultades en la línea de transmisión limitarán el valor de M.

FÓRMULA PARA LA CAPACIDAD DE SHANNON

La fórmula de Nyquist implica que al duplicar el ancho de banda se duplica la velocidad de transmisión, si todo lo demás se mantiene inalterado. Ahora establezcamos una relación entre la velocidad de transmisión, el ruido y la tasa de errores. La presencia de ruido puede corromper uno o más bits. Si se aumenta la velocidad de transmisión, el bit se hace más «corto», de tal manera que dado un patrón de ruido, éste afectará a un mayor número de bits. Así pues, dado un nivel de ruido, cuanto mayor es la velocidad de transmisión, mayor es la tasa de errores.

La Figura 3.16 ilustra esta relación. Si se incrementa la velocidad de transmisión de los datos, entonces habrá más bits durante el intervalo de duración del ruido y, por tanto, habrá un mayor número de errores.

Todos estos conceptos se han relacionado en la fórmula desarrollada por el matemático Claude Shannon. Como se ha comentado, cuanto mayor es la velocidad de transmisión, mayor es el daño que puede ocasionar el ruido. Dado un nivel de ruido, es de esperar que incrementando la energía de la señal se mejoraría la recepción de datos en presencia de ruido. Un parámetro fundamental en el desarrollo de este razonamiento es la relación señal-ruido (SNR, o S/N)[9], que se define como el cociente de la potencia de la señal entre la potencia del ruido presente en un punto determinado en el medio de transmisión. Generalmente, este cociente se mide en el receptor, ya que es aquí donde se realiza el procesado de la señal y la eliminación del ruido no deseado. Por cuestiones de comodidad, la SNR se expresa en decibelios:

$$\text{SNR}_{\text{dB}} = 10 \log_{10} \frac{\text{potencia de señal}}{\text{potencia de ruido}}$$

Esta expresión muestra, en decibelios, cuánto excede la señal al nivel de ruido. Una SNR alta significará una señal de alta calidad y, por tanto, la necesidad de un número reducido de repetidores.

La relación señal-ruido es importante en la transmisión de datos digitales, ya que ésta determina la máxima velocidad de transmisión que se puede conseguir. Una conclusión de Shannon es que la capacidad máxima del canal, en bits por segundo, verifica la ecuación

$$C = B \log_2 (1 + \text{SNR}) \tag{2.1}$$

donde C es la capacidad del canal en bits por segundo y B es el ancho de banda del canal en hercios. La fórmula de Shannon representa el máximo límite teórico que se puede conseguir. Sin embargo, en la práctica, se consiguen velocidades mucho menores. Una razón para esto reside en el hecho de que la fórmula anterior supone ruido blanco (ruido térmico). Además, no se han tenido en cuenta el ruido impulsivo, la distorsión de atenuación o la distorsión de retardo.

La capacidad, tal y como se ha calculado en la fórmula precedente, se denomina capacidad libre de errores. Shannon probó que si la velocidad de información real en el canal es menor que la capacidad libre de errores, entonces es teóricamente posible encontrar una codificación de la señal que consiga una transmisión exenta de errores a través del canal. Desafortunadamente, el teorema de Shannon no sugiere la manera de encontrar dicho código, pero proporciona un criterio de referencia con el que se pueden comparar las prestaciones de los esquemas de comunicación reales.

Pueden ser instructivas otras consideraciones adicionales que se deducen a partir de la ecuación anterior. Para un nivel de ruido dado, podría parecer que la velocidad de transmisión se puede aumentar incrementando tanto la energía de la señal como el ancho de banda. Sin embargo, al aumentar la energía de la señal, también lo hacen las no linealidades del sistema, dando lugar a un aumento del ruido de intermodulación. Obsérvese igualmente que, como el ruido se ha supuesto blanco, cuanto mayor sea el ancho de banda, más ruido se introducirá en el sistema. Por tanto, cuando B aumenta, la SNR disminuye.

[9] En todo el texto, a menos que se indique lo contrario, $\log(x)$ significa $\log_{10}(x)$.

Ejemplo 3.3. En el siguiente ejemplo se relacionan las formulaciones de Shannon y Nyquist. Supóngase que el espectro de un canal está situado entre 3 MHz y 4 MHz y que la $\text{SNR}_{\text{dB}} = 24$ dB. En este caso,

$$B = 4 \text{ MHz} - 3 \text{ MHz} = 1 \text{ MHz}$$
$$\text{SNR}_{\text{dB}} = 24 \text{ dB} = 10 \log_{10}(\text{SNR})$$
$$\text{SNR} = 251$$

Usando la fórmula de Shannon se tiene que

$$C = 10^6 \times \log_2(1 + 251) \approx 10^6 \times 8 = 8 \text{ Mbps}$$

Éste es, como ya se ha mencionado, un límite teórico difícil de alcanzar. No obstante, supóngase que este límite se puede alcanzar. Según la fórmula de Nyquist, ¿cuántos niveles de señalización se necesitarán? Se tiene que

$$C = 2B \log_2 M$$
$$8 \times 10^6 = 2 \times (10^6) \times \log_2 M$$
$$4 = \log_2 M$$
$$M = 16$$

EL COCIENTE E_b/N_0

Finalmente, en este apartado se presenta un parámetro relacionado con la SNR que es más adecuado para determinar las tasas de error y la velocidad de transmisión. Además se usa habitualmente para medir la calidad de las prestaciones de los sistemas de comunicación digital. Este parámetro es el cociente de la energía de la señal por bit entre la densidad de potencia del ruido por hercio, E_b/N_0. Sea una señal, digital o analógica, que contenga datos digitales binarios transmitidos a una determinada velocidad R. Teniendo en cuenta que 1 W = 1 J/s, la energía por bit de la señal será $E_b = ST_b$, donde S es la potencia de la señal y T_b es el tiempo necesario para transmitir un bit. La velocidad de transmisión es $R = 1/T_b$. Por tanto,

$$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR}$$

o, expresado en decibelios,

$$\left(\frac{E_b}{N_0}\right)_{\text{dB}} = S_{\text{dBW}} - 10 \log R - 10 \log k - 10 \log T$$
$$= S_{\text{dBW}} - 10 \log R + 228{,}6 \text{ dBW} - 10 \log T$$

El cociente E_b/N_0 es importante ya que para los datos digitales la tasa de error por bit es una función (decreciente) de este cociente. Dado un valor de E_b/N_0 necesario para conseguir una tasa de errores deseada, los parámetros se pueden seleccionar de acuerdo con la fórmula anterior. Nótese que cuando se aumenta la velocidad de transmisión R, la potencia de la señal transmitida, relativa al ruido, debe aumentarse para mantener el cociente E_b/N_0 requerido.

Intentemos inferir intuitivamente este resultado a partir de la Figura 3.16. La señal aquí considerada es digital, pero el mismo razonamiento podría extenderse para el caso de una señal analógica. En algunos casos, el ruido es suficiente como para alterar el valor de un bit. Ahora, si la velocidad de transmisión se duplicase, los bits tendrían asociada una duración menor, con lo que el mismo ruido podría destruir dos bits. Por tanto, para una señal y ruido de energías constantes, un incremento en la velocidad de transmisión aumentaría la tasa de error.

La ventaja del cociente E_b/N_0 sobre la SNR es que esta última depende del ancho de banda.

Ejemplo 3.4. En la modulación digital binaria PSK (*Phase-Shift Keying*) (definida en el Capítulo 5), para obtener una tasa de error por bit igual a 10^{-4} (un bit erróneo cada 10.000) se necesita un cociente $E_b/N_0 = 8{,}4$ dB. Si la temperatura efectiva es 290 °K (temperatura ambiente) y la velocidad de transmisión es 2.400 bps, ¿qué nivel de señal recibida se necesita?

En este caso se tiene que

$$\begin{aligned} 8{,}4 &= S(\text{dBW}) - 10\log 2.400 + 228{,}6\ \text{dBW} - 10\log 290 \\ &= S(\text{dBW}) - (10)(3{,}38) + 228{,}6 - (10)(2{,}46) \\ S &= -161{,}8\ \text{dBW} \end{aligned}$$

Se puede establecer la relación entre E_b/N_0 y la SNR de la siguiente manera. Se tiene que

$$\frac{E_b}{N_0} = \frac{S}{N_0 R}$$

El parámetro N_0 es la densidad de potencia del ruido en vatios/hercio. Por tanto, el ruido en una señal con ancho de banda B_T es $N = N_0 B_T$. Sustituyendo, se tiene que

$$\frac{E_b}{N_0} = \frac{S}{N}\frac{B_T}{R} \tag{2.2}$$

Otra formulación de interés es la relación entre la eficiencia espectral y E_b/N_0. La fórmula de Shannon [Ecuación (2.1)] se puede rescribir como

$$\frac{S}{N} = 2^{C/B} - 1$$

Usando la Ecuación (2.2), igualando B_T con B y R con C, tenemos que

$$\frac{E_b}{N_0} = \frac{B}{C}(2^{C/B} - 1)$$

Ésta es una fórmula útil que relaciona la eficiencia espectral alcanzable C/B con E_b/N_0.

Ejemplo 3.5. Supóngase que queremos encontrar el máximo E_b/N_0 necesario para conseguir una eficiencia espectral de 6 bps/Hz. Entonces $E_b/N_0 = (1/6)(2^6 - 1) = 10{,}5 = 10{,}21$ dB.

3.5. LECTURAS RECOMENDADAS

Hay muchos libros que cubren los aspectos fundamentales de la transmisión analógica y digital. [COUC97] es bastante completo. Una referencia de calidad es [FREE99], en la que se incluyen algunos de los ejemplos proporcionados a lo largo de este capítulo, y [HAYK01].

COUC01 Couch, L. *Digital and Analog Communicastions Systems*. Upper Saddle River, NJ: Prentice Hall, 2001.

FREE99 Freeman, R. *Fundamentals of Telecommunications*. New York: Wiley, 1999.

HAYK01 Haykin, S. *Communication Systems*. New York: Wiley, 2001.

3.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

amplitud de pico
ancho de banda
ancho de banda absoluto
ancho de banda efectivo
aperiódico
atenuación
capacidad del canal
componente dc
dato
dato analógico
datos digitales
decibelio (dB)
diafonía
distorsión de atenuación
distorsión de retardo
dominio de la frecuencia
dominio del tiempo
enlace directo
enlace multipunto
enlace punto-a-punto
espectro
fase
frecuencia
frecuencia central
frecuencia fundamental
full-duplex
half-duplex
inalámbrico
longitud de onda
medio guiado
medio no guiado
periodo
ruido
ruido de intermodulación
ruido impulsivo
ruido térmico
señal
señal analógica
señal digital
señal periódica
señalización
simplex
transmisión
transmisión analógica
transmisión digital

CUESTIONES DE REPASO

3.1. ¿En qué se diferencia un medio guiado de un medio no guiado?

3.2. ¿Cuáles son las diferencias entre una señal electromagnética analógica y una digital?

3.3. ¿Cuáles son las tres características más importantes de una señal periódica?

3.4. ¿Cuántos radianes hay en 360^{o}?

3.5. ¿Cuál es la relación entre la longitud de onda y la frecuencia en una onda seno?

3.6. ¿Cuál es la relación entre el espectro de una señal y su ancho de banda?

3.7. ¿Qué es la atenuación?

3.8. Defina la capacidad de un canal.

3.9. ¿Qué factores clave afectan a la capacidad de un canal?

EJERCICIOS

3.1. **a)** En una configuración multipunto, sólo un dispositivo puede trasmitir cada vez, ¿por qué?

b) Hay dos posibles aproximaciones que refuerzan la idea de que, en un momento dado, sólo un dispositivo puede transmitir. En un sistema centralizado, una estación es la responsable del control y podrá transmitir o decidir que lo haga cualquier otra. En el método descentralizado, las estaciones cooperan entre sí, estableciéndose una serie de turnos. ¿Qué ventajas y desventajas presentan ambas aproximaciones?

3.2. Una señal tiene una frecuencia fundamental de 1000 Hz. ¿Cuál es su periodo?

3.3. Simplifique las siguientes expresiones:

a) $\text{sen}\,(2\pi ft - \pi) + \text{sen}\,(2\pi ft + \pi)$

b) $\text{sen}\,2\pi ft + \text{sen}\,(2\pi ft - \pi)$

3.4. El sonido se puede modelar mediante funciones sinusoidales. Compare la frecuencia relativa y la longitud de onda de las notas musicales. Piense que la velocidad del sonido es igual a 330 m/s y que las frecuencias de una escala musical son:

Nota	DO	RE	MI	FA	SOL	LA	SI	DO
Frecuencia	264	297	330	352	396	440	495	528

3.5. Si la curva trazada con una línea continua de la Figura 3.17 representa al $\text{sen}\,(2\pi t)$, ¿qué función corresponde a la línea discontinua? En otras palabras, la línea discontinua se puede expresar como $A\,\text{sen}\,(2\pi ft + \phi)$; ¿qué son A, f y ϕ?

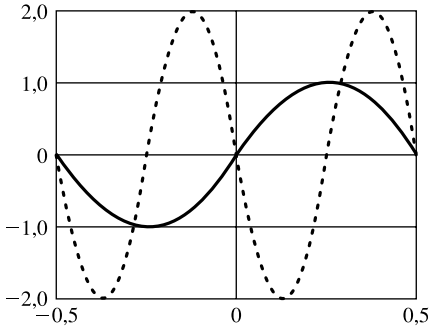


Figura 3.17. Figura del Ejercicio 3.5.

3.6. Exprese la señal $(1 + 0{,}1 \cos 5t) \cos 100t$ como combinación lineal de funciones sinusoidales; encuentre la amplitud, frecuencia y fase de cada una de las componentes. (*Sugerencia:* use la expresión del $\cos a \cos b$).

3.7. Encuentre el periodo de la función $f(t) = (10 \cos t)^2$.

3.8. Sean dos funciones periódicas $f_1(t)$ y $f_2(t)$, con periodos T_1 y T_2 respectivamente. ¿Es periódica la función $f(t) = f_1(t) + f_2(t)$? Si es así, demuéstrelo. Si no, ¿bajo qué condiciones $f(t)$ será periódica?

3.9. La Figura 3.4 muestra el efecto resultante al eliminar las componentes de alta frecuencia de un pulso cuadrado, considerando sólo las componentes de baja frecuencia. ¿Cómo sería la señal resultante en el caso contrario (es decir, quedándose con todos los armónicos de frecuencia alta y eliminando los de bajas frecuencias)?

3.10. La Figura 3.5b muestra la función correspondiente a un pulso rectangular en el dominio de la frecuencia. Este pulso puede corresponder a un 1 digital en un sistema de comunicación. Obsérvese que se necesita un número infinito de frecuencias (con amplitud decreciente cuanto mayor es la frecuencia). ¿Qué implicaciones tiene este hecho en un sistema de transmisión real?

3.11. El IRA es un código de 7 bits que permite la definición de 128 caracteres. En los años setenta, muchos medios de comunicación recibían las noticias a través de un servicio que usaba 6 bits denominado TTS. Este código transmitía caracteres en mayúsculas y minúsculas, así como caracteres especiales y órdenes de control. Generalmente, se utilizan 100 caracteres. ¿Cómo cree que se puede conseguir esto?

3.12. ¿Cuál es el incremento posible en la resolución horizontal para una señal de vídeo de ancho de banda 5 MHz? ¿Y para la resolución vertical? Responda ambas cuestiones por separado; es decir, utilice el incremento de ancho de banda para aumentar la resolución horizontal o la vertical, pero no ambas.

3.13. **a)** Suponga que se transmite una imagen digitalizada de TV de 480 × 500 puntos, en la que cada punto puede tomar uno de entre 32 posibles valores de intensidad. Supóngase que se envían 30 imágenes por segundo (esta fuente digital es aproximadamente igual que los estándares adoptados para la difusión de TV). Determine la velocidad de transmisión R de la fuente en bps.

b) Suponga que la fuente anterior se transmite por un canal de 4,5 MHz de ancho de banda con una relación señal-ruido de 35 dB. Encuentre la capacidad del canal en bps.

c) ¿Cómo se deberían modificar los parámetros del apartado (a) para permitir la transmisión de la señal de TV en color sin incrementar el valor de R?

3.14. Dado un amplificador con una temperatura efectiva de ruido de 10.000 °K y con un ancho de banda de 10 MHz, ¿cuánto será el nivel de ruido térmico a la salida?

3.15. ¿Cuál es la capacidad para un canal de un «teletipo» de 300 Hz de ancho de banda con una relación señal-ruido de 3 dB?

3.16. Para operar a 9.600 bps se usa un sistema de señalización digital:

a) Si cada elemento de señal codifica una palabra de 4 bits, ¿cuál es el ancho de banda mínimo necesario?

b) ¿Y para palabras de 8 bits?

3.17. ¿Cuál es el nivel de ruido térmico para un canal de ancho de banda de 10 kHz y 1000 W de potencia operando a 50 °C?

3.18. Considérense los trabajos de Shannon y Nyquist sobre la capacidad del canal. Cada uno de ellos estableció un límite superior para la razón de bits del canal basándose en dos aproximaciones diferentes. ¿Cómo se pueden relacionar ambas aproximaciones?

3.19. Sea un canal con una capacidad de 20 Mbps. El ancho de banda de dicho canal es 3 MHz. ¿Cuál es la relación señal-ruido admisible para conseguir la mencionada capacidad?

3.20. La onda cuadrada de la Figura 3.7c, con $T = 1$ ms, se transmite a través de un filtro paso bajo ideal de ganancia unidad con frecuencia de corte a 8 kHz.

a) Determine la potencia de la señal de salida.

b) Suponiendo que a la entrada del filtro hay un ruido térmico con $N_0 = 0{,}1$ μW/Hz, encuentre la relación señal-ruido en dB a la salida.

3.21. Si el nivel recibido de una señal en un sistema digital es de -151 dBW y la temperatura efectiva del ruido en el receptor es de 1.500 K, ¿cuánto es el cociente E_b/N_0 para un enlace que transmita a 2.400 bps?

3.22. Rellene las casillas vacías de la siguiente tabla correspondientes a distintas potencias necesarias para obtener la correspondiente relación expresada en decibelios.

Decibelios	1	2	3	4	5	6	7	8	9	10
Pérdidas			0,5							0,1
Ganancias			2							10

3.23. Si un amplificador tiene una ganancia en tensión de 30 dB, ¿cuál es su relación de tensiones de entrada y salida?

3.24. Si un amplificador proporciona a la salida 20 W, ¿cuánto proporcionará expresado en dBW?

APÉNDICE 3A. DECIBELIOS Y ENERGÍA DE LA SEÑAL

Un parámetro importante en cualquier sistema de transmisión es la energía de la señal transmitida. Al propagarse la señal en el medio habrá una pérdida, o *atenuación*, de energía de la señal. Para compensar este hecho es necesario introducir amplificadores cada cierta distancia que restituyan la energía de la señal.

Los valores de ganancias, pérdidas y, en general, de todas las magnitudes relativas se suelen expresar en decibelios, ya que:

- La energía de la señal decae, por lo general, exponencialmente. Por tanto, las pérdidas se pueden expresar cómodamente en decibelios, ya que es una unidad logarítmica.
- En un sistema de transmisión, las ganancias y pérdidas en cascada se pueden calcular fácilmente mediante sumas o restas, respectivamente.

El decibelio es una medida del cociente o proporción entre dos niveles de la señal:

$$G_{\text{dB}} = 10 \log_{10} \frac{P_{\text{salida}}}{P_{\text{entrada}}}$$

donde

N_{dB} = número de decibelios.
$P_{entrada}$ = potencia de entrada.
P_{salida} = potencia de salida.
$\log_{10}$ = logaritmo en base 10.

La Tabla 3.2 muestra varias potencias de 10 expresadas en decibelios.

En la bibliografía hay algunas inconsistencias a la hora de usar los términos *ganancia* y *pérdida*. Si un valor G_{dB} es positivo, corresponde en realidad a una ganancia en potencia. Por ejemplo, una ganancia de 3 dB significa que la potencia se ha doblado. Si el valor de G_{dB} es negativo, en realidad implica una pérdida de potencia. Por ejemplo, una ganancia de -3 dB, significa que la potencia se ha dividido por la mitad, es decir, es una pérdida de potencia. Normalmente eso se expresa diciendo que ha habido una pérdida de 3 dB. Sin embargo, algunas referencias dirían que ha habido una pérdida de -3dB. Tiene más sentido decir que una ganancia negativa corresponde a una pérdida positiva. Por tanto, definimos la pérdida en decibelios L_{dB}, como

$$L_{dB} = -10\log_{10}\frac{P_{salida}}{P_{entrada}} = 10\log_{10}\frac{P_{entrada}}{P_{salida}} \tag{2.2}$$

Tabla 3.2. Valores en decibelios.

Cociente de potencias	dB	Cociente de potencias	dB
10^1	10	10^{-1}	-10
10^2	20	10^{-2}	-20
10^3	30	10^{-3}	-30
10^4	40	10^{-4}	-40
10^5	50	10^{-5}	-50
10^6	60	10^{-6}	-60

Ejemplo 3.6. Si en una línea de transmisión se transmite una señal con una potencia de 10 mW y a cierta distancia se miden 5 mW, la pérdida se puede expresar como $L_{dB} = 10\log(10/5) = 10(0{,}3) = 3$ dB.

Obsérvese que el decibelio es una medida de una diferencia relativa, es decir, no es absoluta. Una pérdida de 1.000 W a 500 W es igualmente una pérdida de 3 dB.

El decibelio también se usa para medir diferencias de tensión, ya que la potencia es proporcional al cuadrado de la tensión:

$$P = \frac{V^2}{R}$$

donde

P = potencia disipada en una resistencia R.

V = caída de tensión en la resistencia R.

Por tanto,

$$L_{\text{dB}} = 10 \log \frac{P_{\text{entrada}}}{P_{\text{salida}}} = 10 \log \frac{V^2_{\text{entrada}}/R}{V^2_{\text{salida}}/R} = 20 \log \frac{V_{\text{entrada}}}{V_{\text{salida}}}$$

Ejemplo 3.7. Los decibelios son útiles para determinar la ganancia o pérdida acumulada por una serie de elementos de transmisión. Sea un conjunto de elementos atacados por una potencia de entrada igual a 4 mW. Sea el primer elemento una línea de transmisión con 12 dB de atenuación (-12 dB de ganancia), el segundo elemento un amplificador con una ganancia igual a 35 dB y, por último, una línea de transmisión con 10 dB de pérdida. La ganancia o atenuación neta será $(-12 + 35 - 10) = 13$ dB. El cálculo de la potencia de salida P_{salida} es,

$$G_{\text{dB}} = 13 = 10 \log (P_{\text{salida}}/4 \text{ mW})$$
$$P_{\text{salida}} = 4 \times 10^{1,3} \text{ mW} = 79,8 \text{ MW}$$

Los valores en decibelios se refieren a magnitudes relativas a cambios en magnitud, no a valores absolutos. A veces es conveniente expresar un nivel absoluto de potencia o tensión en decibelios para facilitar así el cálculo de la pérdida o ganancia con respecto a un valor inicial de señal. El **dBW (decibelio-vatio)** se usa frecuentemente en aplicaciones de microondas. Se elige como referencia el valor de 1 W y se define como 0 dBW. Se define, por tanto, el nivel absoluto de potencia en dBW como

$$\text{Potencia}_{\text{dBW}} = 10 \log \frac{\text{Potencia}_{\text{W}}}{1 \text{ W}}$$

Ejemplo 3.8. Una potencia de 1.000 W corresponde a 30 dBW y una potencia de 1 mW corresponde a -30 dBW.

Otra unidad es el **dBm (decibelio-milivatio),** en la que se usa 1 mW como referencia. Así 0 dBM = 1 mW. La fórmula es

$$\text{Potencia}_{\text{dBW}} = 10 \log \frac{\text{Potencia}_{\text{mW}}}{1 \text{ mW}}$$

Obsérvense las siguientes relaciones

$$+30 \text{ dBm} = 0 \text{ dBW}$$
$$0 \text{ dBm} = -30 \text{ dBW}$$

Otra unidad frecuente en los sistemas de televisión por cable y en las aplicaciones LAN de banda ancha es el **dBmV (decibelio-milivoltio).** Ésta es una medida absoluta, donde 0 dBmV equivale a 1 mV. Por tanto,

$$\text{Tensión}_{\text{dBmV}} = 20 \log \frac{\text{Tensión}_{\text{mV}}}{1 \text{ mV}}$$

En este caso se ha supuesto que la caída de tensión se realiza en una resistencia de 75 ohmios.

CAPÍTULO 4

Medios de transmisión

4.1. Medios de transmisión guiados
Par trenzado
Cable coaxial
Fibra óptica

4.2. Transmisión inalámbrica
Antenas
Microondas terrestres
Microondas por satélite
Ondas de radio
Infrarrojos

4.3. Propagación inalámbrica
Propagación superficial de ondas
Propagación aérea de ondas
Propagación en la trayectoria visual

4.4. Transmisión en la trayectoria visual
Pérdida en el espacio libre
Absorción atmosférica
Multitrayectorias
Refracción

4.5. Lecturas recomendadas y sitios web

4.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- Los medios de transmisión se pueden clasificar como guiados y no guiados. Los medios guiados proporcionan un camino físico a través del cual se propaga la señal; entre éstos están el par trenzado, el cable coaxial y la fibra óptica. Los medios no guiados utilizan una antena para transmitir a través del aire, el vacío o el agua.
- Tradicionalmente, el par trenzado ha sido el medio por excelencia utilizado en las comunicaciones de cualquier tipo. Con el cable coaxial se pueden obtener mayores velocidades de transmisión para mayores distancias. Por esta razón, el coaxial se ha utilizado en redes de área local de alta velocidad y en aplicaciones de enlaces troncales de alta capacidad. No obstante, la capacidad tremenda de la fibra óptica la hace más atractiva que el coaxial y, en consecuencia, la fibra ha copado la mayor parte del mercado de las LAN de alta velocidad y las aplicaciones a larga distancia.
- La emisión por radio, las microondas terrestres y los satélites son las técnicas que se utilizan en la transmisión no guiada. La transmisión por infrarrojos se utiliza en algunas aplicaciones LAN.

En los los sistemas de transmisión de datos, **el medio de transmisión** es el camino físico entre el transmisor y el receptor. Según se estudió en el Capítulo 3, en los **medios guiados** las ondas electromagnéticas se transmiten a través de un medio sólido, como por ejemplo un par trenzado de cobre, un cable coaxial o una fibra óptica. En los medios no guiados, la transmisión inalámbrica se realiza a través de la atmósfera, el espacio exterior o el agua.

Las características y calidad de la transmisión están determinadas tanto por el tipo de señal como por las características del medio. En el caso de los medios guiados, el medio, en sí mismo, es lo que más limitaciones impone a la transmisión.

En medios no guiados, las características de la transmisión están más determinadas por el ancho de banda de la señal emitida por la antena que por el propio medio. Una propiedad fundamental de las señales transmitidas mediante antenas es la direccionalidad. En general, a frecuencias bajas las señales son omnidireccionales; es decir, la señal desde la antena se emite y propaga en todas direcciones. A frecuencias más altas, es posible concentrar la señal en un haz direccional.

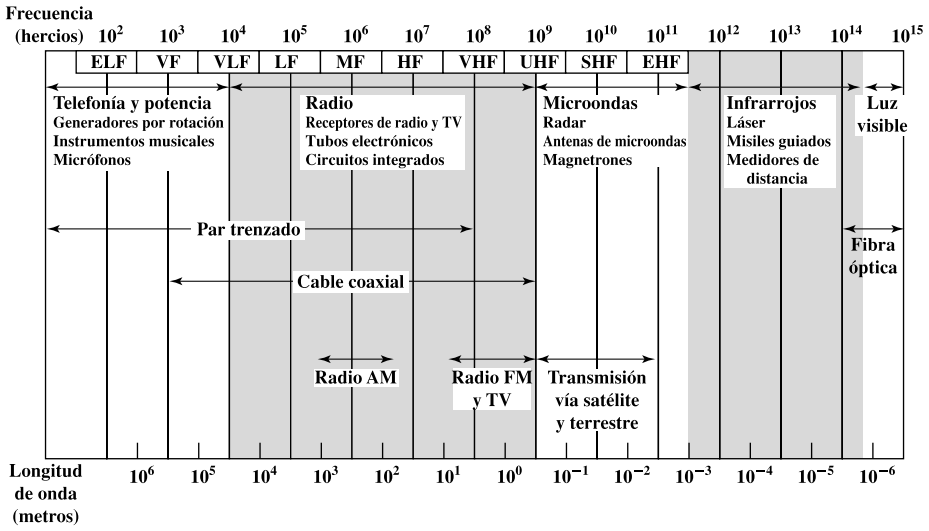
En el diseño de sistemas de transmisión es deseable que tanto la distancia como la velocidad de transmisión sean lo más grandes posibles. Hay una serie de factores relacionados con el medio de transmisión y con la señal que determinan tanto la distancia como la velocidad de transmisión:

- **El ancho de banda:** si todos los otros factores se mantienen constantes, al aumentar el ancho de banda de la señal, la velocidad de transmisión se puede incrementar.
- **Dificultades en la transmisión:** las dificultades, como por ejemplo la atenuación, limitan la distancia. En los medios guiados, el par trenzado sufre de mayores adversidades que el cable coaxial que, a su vez, es más vulnerable que la fibra óptica.
- **Interferencias:** las interferencias resultantes de la presencia de señales en bandas de frecuencias próximas pueden distorsionar o destruir la señal. Las interferencias son especialmente relevantes en los medios no guiados, pero a la vez son un problema a considerar en los medios guiados. En medios guiados, las emisiones de cables cercanos pueden causar interferencias. Así, por ejemplo, es frecuente embutir múltiples cables de pares trenzados dentro de

una misma cubierta. Las interferencias también pueden aparecer en las transmisiones no guiadas. Un apantallamiento adecuado del medio guiado puede minimizar este problema.

- **Número de receptores:** un medio guiado se puede usar tanto para un enlace punto a punto como para un enlace compartido, mediante el uso de múltiples conectores. En este último caso, cada uno de los conectores utilizados puede atenuar y distorsionar la señal, por lo que la distancia y/o la velocidad de transmisión disminuirán.

En la Figura 4.1 se muestra el espectro electromagnético, así como la frecuencia a la que operan diferentes técnicas de transmisión sobre medios guiados y no guiados. En este capítulo se estudiarán las diferentes alternativas tanto para medios guiados como para no guiados. En todos los casos, se describirán físicamente los sistemas, se discutirán brevemente las aplicaciones y se resumirán las características principales de transmisión.



ELF (*Extremely low frequency*) = Frecuencia extremadamente baja
VF (*Voice frequency*) = Frecuencia vocal
VLF (*Very low frequency*) = Frecuencia muy baja
LF (*Low frequency*) = Frecuencia baja
MF (*Medium frequency*) = Frecuencia media
HF (*High frequency*) = Frecuencia alta
VHF (*Very high frequency*) = Frecuencia muy alta
UHF (*Ultrahigh frequency*) = Frecuencia ultra alta
SHF (*Superhigh frequency*) = Frecuencia super alta
EHF (*Extremely high frequency*) = Frecuencia extremadamente alta

Figura 4.1. Espectro electromagnético para las telecomunicaciones.

4.1. MEDIOS DE TRANSMISIÓN GUIADOS

En los medios de transmisión guiados, la capacidad de transmisión, en términos de velocidad de transmisión o ancho de banda, depende drásticamente de la distancia y de si el medio es punto a punto o multipunto. En la Tabla 4.1 se indican las características típicas de los medios guiados más comunes para aplicaciones punto a punto de larga distancia. El estudio de la utilización de estos medios en LAN se aplaza para más adelante, a la Parte IV del libro.

Los tres medios guiados que más se utilizan en la transmisión de datos son el par trenzado, el cable coaxial y la fibra óptica (*véase* Figura 4.2). A continuación, examinaremos cada uno de ellos.

Tabla 4.1. Características de transmisión de medios guiados punto-a-punto [GLOV98].

	Rango de frecuencias	Atenuación típica	Retardo típico	Separación entre repetidores
Par trenzado (con carga)	0 para 3,5 kHz	0,2 dB/km @ 1 kHz	50 μs/km	2 km
Pares trenzados (cables multi-pares)	0 para 1 MHz	3 dB/km @ 1 kHz	5 μs/km	2 km
Cable coaxial	0 para 500 MHz	7 dB/km @ 10 MHz	4 μs/km	1 a 9 km
Fibra óptica	180 para 370 THz	0,2 a 0,5 dB/km	5 μs/km	40 km

THz = Terahercios = 10^{12} Hz.

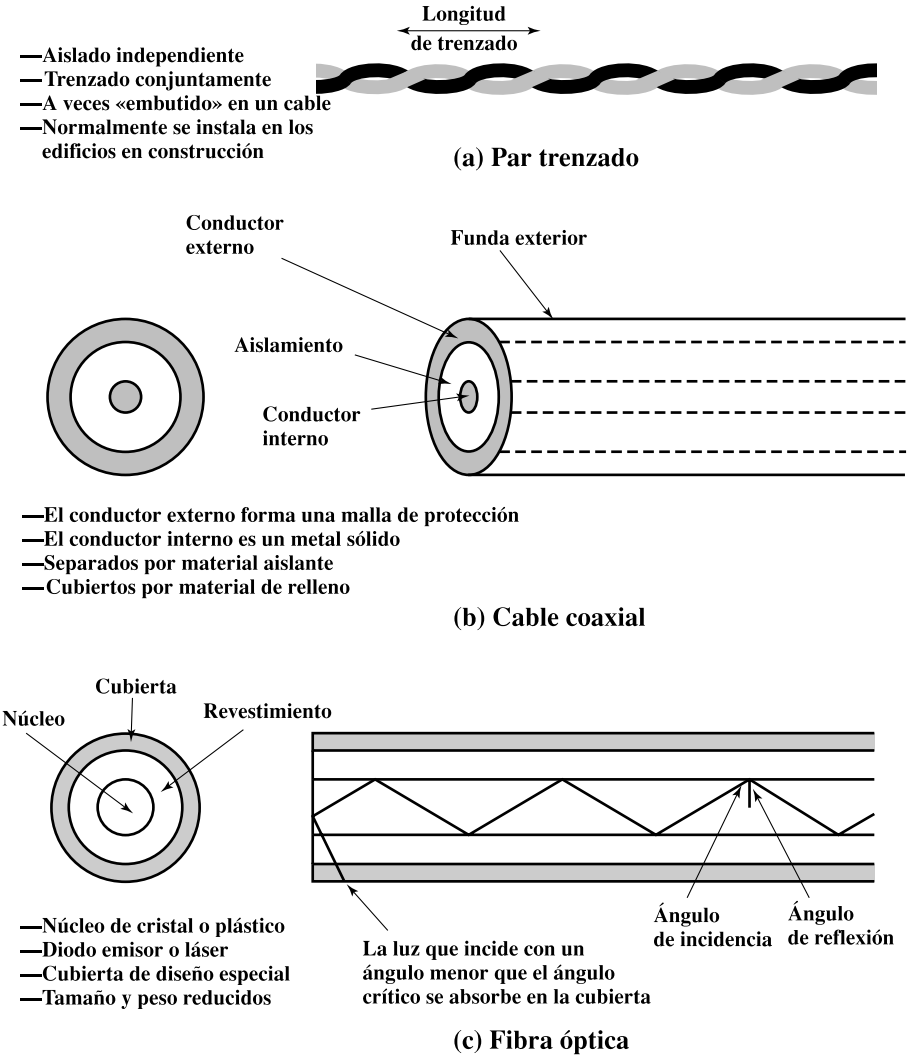


Figura 4.2. Medios de transmisión guiados.

PAR TRENZADO

El par trenzado es el medio guiado más económico y, a la vez, es el más usado.

Descripción física

El par trenzado consiste en dos cables de cobre embutidos en un aislante, entrecruzados en forma de bucle espiral. Cada par de cables constituye un enlace de comunicación. Normalmente, varios pares se encapsulan conjuntamente mediante una envoltura protectora. En el caso de largas distancias, la envoltura puede contener cientos de pares. El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. Para este fin, los pares adyacentes dentro de una misma envoltura se trenzan con pasos de torsión diferentes. En enlaces de larga distancia, la longitud del trenzado varía entre 5 cm y 15 cm. Los conductores que forman el par tienen un grosor que varía entre 0,4 mm y 0,9 mm.

Aplicaciones

Tanto para señales analógicas como para señales digitales, el par trenzado es con diferencia el medio de transmisión más usado. El par trenzado es el medio más usado en las redes de telefonía e, igualmente, su uso es básico en el tendido de redes de comunicación dentro de edificios.

En telefonía, el terminal de abonado se conecta a la central local, también denominada «central final», mediante cable de par trenzado, denominado **bucle de abonado**. Igualmente, dentro de los edificios de oficinas, cada teléfono se conecta mediante par trenzado a la central privada (PBX, *Private Branch Exchange*). Estas instalaciones de pares trenzados se diseñaron para transportar tráfico de voz mediante señalización analógica. No obstante, con el uso de los módem, esta infraestructura puede utilizarse para transportar tráfico digital a velocidades de transmisión reducidas.

En la señalización digital, el par trenzado es, igualmente, el más utilizado. Es habitual que los pares trenzados se utilicen para las conexiones al conmutador digital o a la PBX digital a velocidades de 64 Kbps. El par trenzado también se utiliza, dentro de edificios, como medio de transmisión para las redes de área local. La velocidad típica en este tipo de configuraciones está en torno a los 10 Mbps. No obstante, recientemente se han desarrollado redes de pares trenzados con velocidades de hasta 1 Gbps, aunque estas configuraciones están bastante limitadas en el número de posibles dispositivos a conectar y en la extensión geográfica de la red. Para aplicaciones de larga distancia, el par trenzado se puede utilizar a velocidades de 4 Mbps o incluso mayores.

El par trenzado es mucho menos costoso que cualquier otro medio de transmisión guiado (cable coaxial o fibra óptica) y, a la vez, es más sencillo de manejar.

Características de transmisión

El par trenzado se puede usar para transmitir tanto señales analógicas como señales digitales. Al transmitir señales analógicas exige amplificadores cada 5 km o 6 km. Para transmisión digital (usando tanto señales analógicas como digitales), el par requiere repetidores cada 2 km o 3 km.

Comparado con otros medios guiados (como el cable coaxial o la fibra óptica), el par trenzado permite distancias menores, menor ancho de banda y menor velocidad de transmisión. En la Figura 4.3a, se muestra la fuerte dependencia de la atenuación con la frecuencia que presenta el par

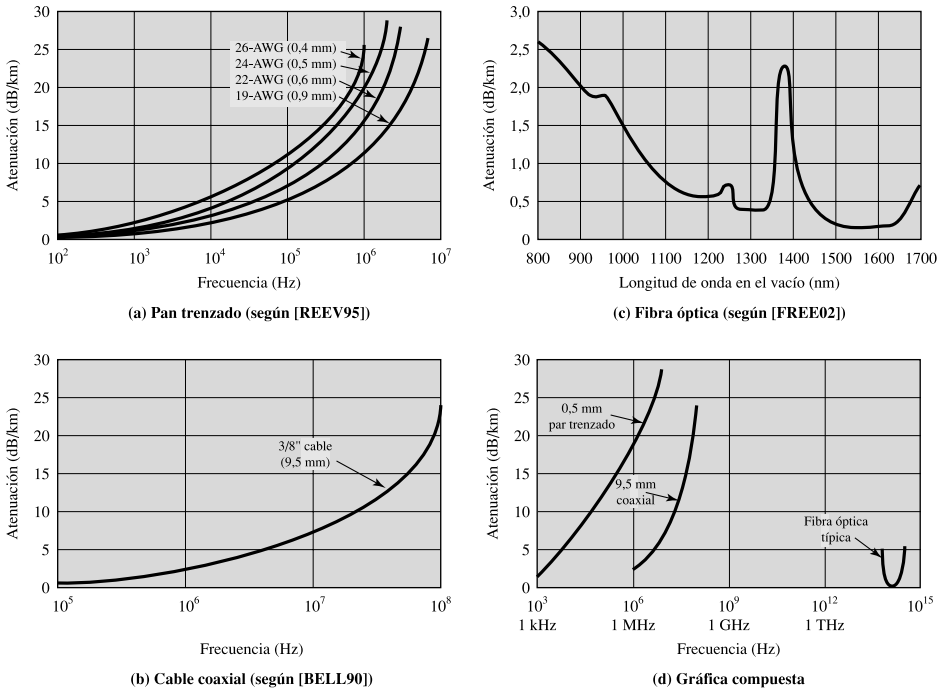


Figura 4.3. Atenuación en los medios guiados típicos.

trenzado. El par es también muy vulnerable a otras dificultades en la transmisión. Este medio se caracteriza por su gran susceptibilidad a las interferencias y al ruido, debido a su fácil acoplamiento con campos electromagnéticos externos. Así, por ejemplo, un cable conductor situado en paralelo con una línea de potencia que conduzca corriente alterna captará energía con una frecuencia de 60 Hz[1]. El ruido impulsivo también afecta a los pares trenzados. Para reducir estos efectos negativos es posible tomar algunas medidas. Por ejemplo, el apantallamiento del cable con una malla metálica reduce las interferencias externas. El trenzado en los cables reduce las interferencias de baja frecuencia y el uso de distintos pasos de torsión entre los pares adyacentes reduce la diafonía.

En sistemas con señalización analógica punto a punto, un par trenzado puede ofrecer hasta 1 MHz de ancho de banda, lo que permite transportar un buen número canales de voz. En el caso de señalización digital punto a punto de larga distancia, se pueden conseguir del orden de unos pocos Mbps; para distancias cortas, ya hay disponibles productos comerciales que proporcionan 1 Gbps.

Pares trenzados apantallados y sin apantallar

Hay dos variantes de pares trenzados: apantallados y sin apantallar. En telefonía, el par trenzado no apantallado (UTP, *Unshielded Twisted Pair*) es el cable más habitual. Es práctica común la preinstalación de par trenzado no apantallado en edificios, aunque normalmente se dimensiona muy por encima de lo que verdaderamente se necesita para el servicio de telefonía. Esto es así porque el par

[1] *N. del T.:* 50 Hz en Europa.

sin apantallar es el menos caro de todos los medios de transmisión que se usan en las redes de área local, además de ser fácil de instalar y manipular.

El par trenzado sin apantallar se puede ver afectado por interferencias electromagnéticas externas, incluyendo interferencias de pares cercanos o fuentes de ruido próximas. Una manera de mejorar las características de transmisión de este medio es embutiéndolo dentro de una malla metálica, reduciéndose así las interferencias. El par trenzado apantallado (STP, *Shielded Twisted Pair*) proporciona mejores prestaciones a velocidades de transmisión superiores. Ahora bien, este último es más costoso y difícil de manipular que el anterior.

UTP tipo 3 y tipo 5

En la mayoría de los edificios de oficinas se hace una preinstalación con par trenzado de 100 ohmios, denominado par de calidad telefónica (*voice-grade*). Es por esto por lo que este tipo de preinstalaciones se deben considerar siempre como una alternativa, bastante atractiva y poco costosa, para ser utilizada como medio de transmisión en las LAN. No obstante, hay que tener en cuenta que las velocidades de transmisión y las distancias que se pueden alcanzar con este medio son limitadas.

En 1991, la EIA (*Electronic Industries Association*) publicó el documento EIA-568, denominado *Estándar para los cables de telecomunicaciones en edificaciones comerciales (Commercial Building Telecommunications Cabling Standard)*, que define el uso de pares trenzados sin apantallar de calidad telefónica y de pares apantallados como medios de transmisión de datos en edificios. Nótese que, por aquel tiempo, las características de dichos medios eran suficientes para el rango de frecuencias y velocidades típicas necesarias en las aplicaciones ofimáticas. Es más, en esa época, las LAN tenían por objetivo velocidades de transmisión comprendidas entre 1 y 16 Mbps. Con el tiempo, los usuarios han migrado a estaciones de trabajo y aplicaciones de mayores prestaciones. Como consecuencia, ha habido un interés creciente en LAN que proporcionen hasta 100 Mbps sobre medios no costosos. Como respuesta a esa necesidad, en 1995 se propuso el EIA-568-A. Esta norma incorpora los avances más recientes, tanto en el diseño de cables y conectores, como en los métodos de test. En esta especificación se consideran cables de pares apantallados a 150 ohmios y pares no apantallados de 100 ohmios.

En el estándar EIA-568-A se consideran tres tipos o categorías de cables UTP:

- **Tipo 3:** cables y hardware asociado, diseñados para frecuencias de hasta 16 MHz.
- **Tipo 4:** cables y hardware asociado, diseñados para frecuencias de hasta 20 MHz.
- **Tipo 5:** cables y hardware asociado, diseñados para frecuencias de hasta 100 MHz.

De entre los anteriores, los tipos 3 y 5 son los más utilizados en los entornos LAN. El tipo 3 coincide con los cables de calidad telefónica que existen en la mayoría de las edificaciones. Con un diseño apropiado y a distancias limitadas, con cables tipo 3 se pueden conseguir velocidades de hasta 16 Mbps. El tipo 5 (*data-grade*) es un cable de mejores características para la transmisión de datos, por lo que cada vez se está utilizando más como preinstalación en los edificios de reciente construcción. Con un diseño apropiado y a distancias limitadas, con cables tipo 5 se pueden alcanzar 100 Mbps.

La diferencia esencial entre los cables tipo 3 y 5 está en el número de trenzas por unidad de longitud. El cable tipo 5 es más trenzado, siendo su paso de trenzado del orden de 0,6 cm a 0,85 cm,

mientras que el tipo 3 tiene una trenza cada 7,5 cm o 10 cm. El trenzado del tipo 5 es por supuesto más caro, ahora bien, proporciona prestaciones superiores que el de tipo 3.

En la Tabla 4.2 se resumen las prestaciones de los mencionados cables: UTP tipo 3 y UTP tipo 5, así como el cable STP especificado en el EIA-568-A. El primer parámetro utilizado en la comparativa es la atenuación. Como es sabido, la energía de la señal decrece con la distancia recorrida en cualquier medio de transmisión. En medios guiados la atenuación obedece a una ley exponencial, por tanto, se expresa normalmente como un número constante de decibelios por unidad de longitud.

Tabla 4.2. Comparativa de pares trenzados apantallados y sin apantallar.

	Atenuación (dB por 100 m)			Diafonía cercana al extremo (dB)		
Frecuencia (MHz)	**UTP tipo 3**	**UTP tipo 5**	**STP 150 ohmios**	**UTP tipo 3**	**UTP tipo 5**	**STP 150 ohmios**
1	2,6	2,0	1,1	41	62	58
4	5,6	4,1	2,2	32	53	58
16	13,1	8,2	4,4	23	44	50,4
25	—	10,4	6,2	—	41	47,5
100	—	22,0	12,3	—	32	38,5
300	—	—	21,4	—	—	31,3

La diafonía denominada *cercana al extremo* es debida a la inducción que provoca un par conductor en otro par cercano. Por conductor debe entenderse tanto los pares que forman el cable como los contactos o «pines» (patillas metálicas) del conector. La denominación *cercana al extremo* hace referencia al acoplamiento que tiene lugar cuando la señal a transmitir entra en el cable y retorna a través del otro par conductor en el mismo extremo del enlace (es decir, la señal transmitida es captada por un par receptor cercano).

Tabla 4.3. Clases y tipos de pares trenzados.

	Tipo 3 Clase C	**Tipo 5 Clase D**	**Clase 5E**	**Tipo 6 Clase E**	**Tipo 7 Clase F**
Ancho de banda	16 MHz	100 MHz	100 MHz	200 MHz	600 MHz
Cable	UTP	UTP/FTP	UTP/FTP	UTP/FT	SSTP
Coste (tipo 5 = 1)	0,7	1	1,2	1,5	2,2

UTP = Par trenzado no apantallado (*Unshielded Twisted Pair*).
FTP = Par trenzado con papel de plata (*Foil Twisted Pair*).
SSTP = Par trenzado tipo 7 (*Shielded-Sreen Twisted Pair*).

Tabla 4.4. Alternativas de altas prestaciones para el cableado de cobre en LAN [JOHN98].

Nombre	Construcción	Prestaciones esperadas	Coste
UTP tipo 5	El cable está constituido por 4 pares de cobre de 0,5 mm con una cubierta termoplástica de poliolefina o de etileno-propileno fluorado (FEP, *Fluorinated Ethylene Propylene*). La funda exterior es de policloruro de vinilo (PVC, *polyvinylchlorides*), una poliolefina ignífuga o un fluoropolímero.	Distintos cables mezclados y acoplados con el hardware de conexión de distintos fabricantes pueden llegar a verificar los requisitos de ISO clase D y de la norma TIA tipo 5. No hay garantía alguna por parte de los fabricantes.	1
UTP tipo 5 mejorado (Clase 5E, *Enhanced*)	El cable está constituido por 4 pares de cobre de 0,5 mm con una cubierta termoplástica de poliolefina o de etileno-propileno fluorado (FEP). La funda exterior es de policloruro de vinilo (PVC), una poliolefina ignífuga o un fluoropolímero. Ha sido fabricado y diseñado con más cuidado.	Los componentes tipo 5 de un suministrador, o de varios, han sido deliberadamente acoplados en impedancia. Ofrecen una ACR mejor que el tipo 5 y la clase D, así como una garantía de 10 años o superior.	1,2
UTP tipo 6	El cable está constituido por 4 pares de cobre de 0,50 a 0,53 mm con una cubierta termoplástica de poliolefina o de etileno-propileno fluorado (FEP). La funda exterior es de policloruro de vinilo (PVC), una poliolefina ignífuga o un fluoropolímero. Ha sido fabricado y diseñado con mucho más cuidado. Los conectores tienen un diseño avanzado.	Los componentes tipo 6 de un fabricante deben estar extremadamente acoplados. Se garantiza así una ACR (ancho de banda efectivo) igual a 0 en el canal para frecuencias iguales a 200 MHz o superiores. Es el mejor UTP disponible. Se está desarrollando la especificación de las prestaciones para el UTP tipo 6 a 250 MHz.	1,5
Par trenzado con papel de plata, FTP (*Foil Twisted Pair*)	El cable está constituido por 4 pares de cobre de 0,5 mm con una cubierta termoplástica de poliolefina o de etileno-propileno fluorado (FEP). Los pares están cubiertos por una malla de papel de plata. La funda exterior es de policloruro de vinilo (PVC), una poliolefina ignífuga o un fluoropolímero.	Los componentes tipo 5 de uno o varios fabricantes se han diseñado expresamente para minimizar la susceptibilidad EMI y para maximizar la inmunidad EMI. Se pueden ofrecer distintas calidades con diversos valores ACR.	1,3
Par trenzado con papel de plata apantallado, SFTP (*Shielded Foil Twisted Pair*)	El cable está constituido por 4 pares de cobre de 0,5 mm con una cubierta termoplástica de poliolefina o de etileno-propileno fluorado (FEP). Los pares están cubiertos por una malla de papel de plata, recubiertos de una malla metálica. La funda exterior es de policloruro de vinilo (PVC), una poliolefina ignífuga o un fluoropolímero.	Los componentes tipo 5 de uno o varios fabricantes deben estar expresamente diseñados para minimizar la susceptibilidad EMI y para maximizar la inmunidad EMI. Ofrece una protección superior a las EMI que el FTP.	1,4
Par trenzado tipo 7, SSTP (*Shielded-Screen Twisted Pair*)	También denominado PiMF (pares en papel de plata, *Pairs in Metal Foil*), el SSTP está constituido por 4 pares de 0,45-0,45 mm pares de cobre con una cubierta termoplástico de poliolefina o de etileno-propileno fluorado (FEP). Los pares están cubiertos individualmente por una malla longitudinal o helicoidal de papel de plata, recubiertos por una malla metálica. La funda exterior es de policloruro de vinilo (PVC) una poliolefina ignífuga o un fluoropolímero.	El cable tipo 7 proporciona ACR positivas entre 600 y 1.200 MHz. El apantallado individual de los pares consigue una ACR extraordinaria.	2,2

ACR = Cociente entre la atenuación y la diafonía (*Attenuation to Crosstalk Ratio*).

EMI = Interferencia electromagnética (*Electromagnetic Interferente*).

CABLE COAXIAL

Descripción física

El cable coaxial, al igual que el par trenzado, tiene dos conductores, pero está construido de forma diferente para que pueda operar sobre un rango de frecuencias mayor. Consiste en un conductor cilíndrico externo que rodea a un cable conductor interior (*véase* Figura 4.2b). El conductor interior se mantiene a lo largo del eje axial mediante una serie de anillos aislantes regularmente espaciados, o bien mediante un material sólido dieléctrico. El conductor exterior se protege con una cubierta o funda. El cable coaxial tiene un diámetro aproximado entre 1 cm y 2,5 cm. Comparado con el par trenzado, el cable coaxial se puede usar para cubrir mayores distancias así como para conectar un número mayor de estaciones en líneas compartidas.

Aplicaciones

El cable coaxial es quizá el medio de transmisión más versátil, por lo que se está utilizando cada vez más en una gran variedad de aplicaciones. Las más importantes son:

- La distribución de televisión.
- La telefonía a larga distancia.
- Los enlaces en computadores a corta distancia.
- Las redes de área local.

El cable coaxial se emplea para la distribución de las señales de *TV por cable* hasta el domicilio de los usuarios. Diseñado inicialmente para proporcionar servicio de televisión a áreas remotas (CATV, *Community Antenna Television*), la TV por cable llega a casi tantos hogares y oficinas como el sistema telefónico. El sistema de TV por cable puede transportar docenas, e incluso cientos de canales, a distancias de hasta varias decenas de kilómetros.

Tradicionalmente, el coaxial ha sido un elemento fundamental en la red de telefonía a larga distancia. En la actualidad tiene una fuerte competencia en la fibra óptica, las microondas terrestres y las comunicaciones vía satélite. Usando multiplexación por división en frecuencia (FDM, *Frequency Division Multiplexing*, *véase* Capítulo 8), el cable coaxial puede transportar simultáneamente más de 10.000 canales de voz.

El cable coaxial también se usa frecuentemente para conexiones entre periféricos o dispositivos a distancias cortas. Usando señalización digital, el coaxial se puede utilizar como medio de transmisión en canales de entrada/salida (E/S) de alta velocidad en computadores.

Características de transmisión

El cable coaxial se usa para transmitir tanto señales analógicas como digitales. Como se puede observar en la Figura 4.3b, el cable coaxial tiene una respuesta en frecuencias mejor que la del par trenzado permitiendo, por tanto, mayores frecuencias y velocidades de transmisión. Debido al apantallamiento, por construcción, el cable coaxial es mucho menos susceptible que el par trenzado tanto a interferencias como a diafonía. Sus principales limitaciones son la atenuación, el ruido térmico y el ruido de intermodulación. Este último aparece sólo cuando sobre el mismo cable se usan simultáneamente varios canales o bandas de frecuencias (FDM).

En la transmisión de señales analógicas a larga distancia se necesitan amplificadores separados entre sí a distancias del orden de pocos kilómetros, siendo esta separación tanto menor cuanto mayor sea la frecuencia de trabajo. El espectro de la señalización analógica se extiende hasta aproximadamente 500 MHz. En la señalización digital, en cambio, se necesita un repetidor cada kilómetro aproximadamente, e incluso menos cuanto mayor sea la velocidad de transmisión.

FIBRA ÓPTICA

Descripción física

La fibra óptica es un medio flexible y delgado (de 2 a 125 μm) capaz de confinar un haz de naturaleza óptica. Para construir la fibra se pueden usar diversos tipos de cristales y plásticos. Las pérdidas menores se han conseguido con la utilización de fibras de silicio ultrapuro fundido. Las fibras ultrapuras son muy difíciles de fabricar; las fibras de cristal multicomponente son más económicas y, aunque sufren mayores pérdidas, proporcionan unas prestaciones suficientes. La fibra de plástico tiene todavía un coste menor, pudiendo ser utilizada en enlaces de distancias más cortas, en los que sean aceptables pérdidas moderadamente altas.

Un cable de fibra óptica tiene forma cilíndrica y está formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta (*véase* Figura 4.2c). El **núcleo** es la sección más interna; está constituido por una o varias fibras de cristal o plástico, con un diámetro entre 8 y 100 μm. Cada fibra está rodeada por su propio **revestimiento**, que no es sino otro cristal o plástico con propiedades ópticas distintas a las del núcleo. La separación entre el núcleo y el revestimiento actúa como un reflector, confinando así el haz de luz, ya que de otra manera escaparía del núcleo. La capa más exterior que envuelve a uno o varios revestimientos es la **cubierta**. La cubierta está hecha de plástico y otros materiales dispuestos en capas para proporcionar protección contra la humedad, la abrasión, posibles aplastamientos y otros peligros.

Aplicaciones

Uno de los avances tecnológicos más significativos y rompedores en la transmisión de datos ha sido el desarrollo de los sistemas de comunicación de fibra óptica. No en vano, la fibra disfruta de una gran aceptación para las telecomunicaciones a larga distancia y, cada vez, está siendo más utilizada en aplicaciones militares. Las mejoras constantes en las prestaciones a precios cada vez inferiores, junto con sus ventajas inherentes, han contribuido decisivamente para que la fibra sea un medio atractivo en los entornos de red de área local. Las características diferenciales de la fibra óptica frente al cable coaxial y al par trenzado son:

- **Mayor capacidad:** el ancho de banda potencial y, por tanto, la velocidad de transmisión, en las fibras es enorme. Experimentalmente se ha demostrado que se pueden conseguir velocidades de transmisión de cientos de Gbps para decenas de kilómetros de distancia. Compárese con el máximo que se puede conseguir en el cable coaxial de cientos de Mbps sobre aproximadamente 1 km, o con los escasos Mbps que se pueden obtener para la misma distancia, o compárese con los 100 Mbps o incluso 1 Gbps para pocas decenas de metros que se consiguen en los pares trenzados.
- **Menor tamaño y peso:** las fibras ópticas son apreciablemente más finas que el cable coaxial o que los pares trenzados embutidos, por lo menos en un orden de magnitud para capacidades de transmisión comparables. En las conducciones o tubos de vacío previstos para el

cableado en las edificaciones, así como en las conducciones públicas subterráneas, la utilización de tamaños pequeños tiene unas ventajas evidentes. La reducción en tamaño lleva a su vez aparejada una reducción en peso que disminuye, a su vez, la infraestructura necesaria.

- **Atenuación menor:** la atenuación es significativamente menor en las fibras ópticas que en los cables coaxiales y pares trenzados (*véase* Figura 4.3c), además, es constante a lo largo de un gran intervalo.
- **Aislamiento electromagnético:** los sistemas de fibra óptica no se ven afectados por los efectos de campos electromagnéticos exteriores. Estos sistemas no son vulnerables a interferencias, ruido impulsivo o diafonía. Por la misma razón, las fibras no radian energía, produciendo interferencias despreciables con otros equipos que proporcionan, a la vez, un alto grado de privacidad; además, relacionado con esto, la fibra es por construcción difícil de «pinchar».
- **Mayor separación entre repetidores:** cuantos menos repetidores haya el coste será menor, además de haber menos fuentes de error. Desde este punto de vista, las prestaciones de los sistemas de fibra óptica han sido mejoradas de manera constante y progresiva. Para la fibra es práctica habitual necesitar repetidores separados entre sí del orden de decenas de kilómetros e, incluso, se han demostrado experimentalmente sistemas con separación de cientos de kilómetros. Por el contrario, los sistemas basados en coaxial y en pares trenzados requieren repetidores cada pocos kilómetros.

Las cinco aplicaciones básicas en las que la fibra óptica es importante son:

- Transmisiones a larga distancia.
- Transmisiones metropolitanas.
- Acceso a áreas rurales.
- Bucles de abonado.
- Redes de área local.

La transmisión a largas distancias mediante fibras es cada vez más común en las redes de telefonía. En estas redes, las distancias medias son aproximadamente 1.500 km; además, se caracterizan por tener una gran capacidad (normalmente de 20.000 a 60.000 canales de voz). En cuanto al coste, estos sistemas son competitivos con los enlaces de microondas; estando tan por debajo, en coste, del cable coaxial que en muchos países desarrollados la fibra está incluso desbancando al coaxial en telefonía. Paralelamente, la fibra óptica cada vez se utiliza más como medio de transmisión en cables submarinos.

Los circuitos troncales en áreas metropolitanas tienen una longitud media de 12 km, pudiendo albergar hasta 100.000 canales de voz por cada grupo troncal. La mayoría de los servicios se están desplegando usando conducciones subterráneas sin repetidores, las cuales se utilizan para enlazar centrales telefónicas dentro del área metropolitana. A esta categoría pertenecen igualmente las rutas que enlazan las líneas de larga distancia de microondas, que llegan hasta las áreas perimetrales de las ciudades, con las centrales de telefonía situadas dentro del casco urbano.

Los accesos a áreas rurales, para enlazar pueblos con ciudades, tienen generalmente longitudes que van desde los 40 a 160 km. En Estados Unidos, estos enlaces a su vez conectan frecuentemente centrales telefónicas pertenecientes a diferentes compañías. La mayoría de estos sistemas tienen menos de 5.000 canales de voz. Normalmente, la tecnología utilizada en estas aplicaciones compite con las microondas.

Los bucles de abonado son fibras que van directamente desde las centrales al abonado. El uso de la fibra en estos servicios esta empezando a desplazar a los enlaces de par trenzado o coaxial, dado que, cada vez más, las redes de telefonía están evolucionando hacia redes integradas capaces de gestionar no sólo voz y datos, sino también imágenes y vídeo. El uso de la fibra en este contexto está encabezado fundamentalmente por grandes clientes (empresas), no obstante, la fibra como medio de acceso desde los domicilios particulares aparecerá en un futuro a corto plazo.

Finalmente, una aplicación importante de la fibra óptica está en las redes de área local. Recientemente, se han desarrollado estándares y productos para redes de fibra óptica con capacidades que van desde 100 Mbps hasta 10 Gbps, las cuales a su vez permiten cientos, incluso miles de estaciones, en grandes edificios de oficinas.

Las ventajas de la fibra óptica respecto del par trenzado o del cable coaxial serán cada vez más convincentes conforme la demanda de información multimedia vaya aumentando (voz, datos, imágenes y vídeo).

Características de transmisión

La fibra óptica propaga internamente el haz de luz que transporta la señal codificada de acuerdo con el principio de **reflexión total**. Este fenómeno se da en cualquier medio transparente que tenga un índice de refracción mayor que el medio que lo contenga. En efecto, la fibra óptica funciona como una guía de ondas para el rango de frecuencias que va desde 10^{14} hasta 10^{15} Hz, cubriendo parte del espectro visible e infrarrojo.

En la Figura 4.4 se muestra el principio que rige la propagación del haz de luz en la fibra óptica. La luz proveniente de la fuente penetra en el núcleo cilíndrico de cristal o plástico. Los rayos que inciden con ángulos superficiales se reflejan y se propagan dentro del núcleo de la fibra, mientras que para otros ángulos de incidencia, los rayos son absorbidos por el material que forma el revestimiento. Este tipo de propagación se llama **multimodal de índice discreto**, aludiendo al hecho de que hay multitud de ángulos para los que se da la reflexión total. En la transmisión

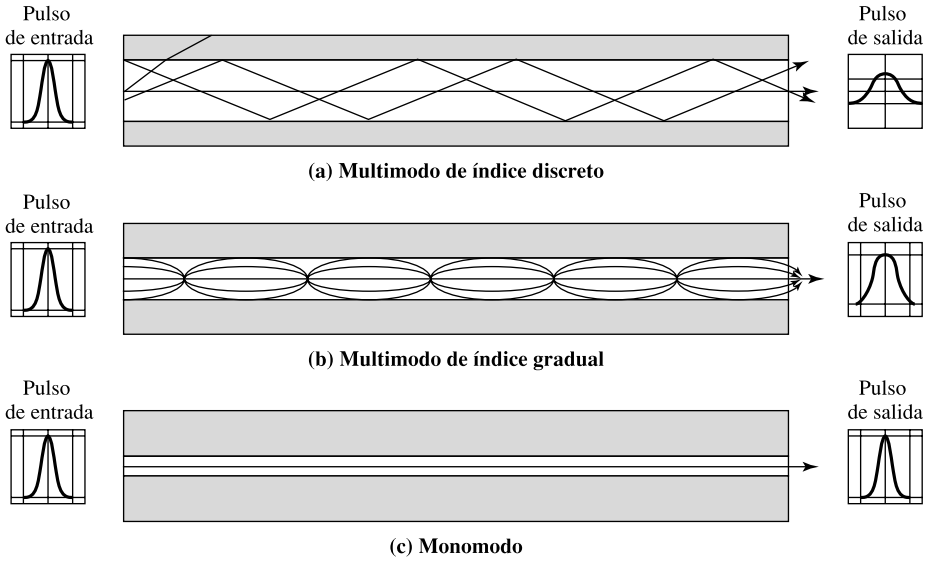


Figura 4.4. Modos de transmisión en las fibras ópticas.

multimodo, existen múltiples caminos que verifican la reflexión total, cada uno con diferente longitud y, por tanto, con diferente tiempo de propagación. Esto hace que los elementos de señalización que se transmitan (los pulsos de luz) se dispersen en el tiempo, limitando así la velocidad a la que los datos puedan ser correctamente recibidos. Dicho de otra forma, la necesidad de separar los pulsos de luz limita la velocidad de transmisión de los datos. Este tipo de fibra es más adecuada para la transmisión a distancias cortas. Cuando el radio del núcleo se reduce, la reflexión total se dará en un número menor de ángulos. Al reducir el radio del núcleo a dimensiones del orden de magnitud de la longitud de onda un solo ángulo, o modo, podrá pasar el rayo axial. Este tipo de propagación, denominada **monomodo,** proporciona prestaciones superiores debido a la existencia de un único camino posible, impidiéndose así la distorsión multimoda. Las fibras monomodo se utilizan generalmente en aplicaciones de larga distancia, por ejemplo en telefonía y televisión por cable. Finalmente, se puede conseguir un tercer modo de transmisión variando gradualmente el índice de refracción del núcleo, este modo se denomina **multimodo de índice gradual**. Las características de este último modo están entre las de los otros dos modos comentados. Estas fibras, al disponer de un índice de refracción superior en la parte central, hacen que los rayos de luz avancen más rápidamente conforme se alejan del eje axial de la fibra. En lugar de describir un zig-zag, la luz en el núcleo describe curvas helicoidales debido a la variación gradual del índice de refracción, reduciendo así la longitud recorrida. El efecto de tener una mayor velocidad de propagación y una longitud inferior posibilita que la luz periférica llegue al receptor al mismo tiempo que los rayos axiales del núcleo. Las fibras de índice gradual se utilizan frecuentemente en las redes de área local.

En los sistemas de fibra óptica se usan dos tipos diferentes de fuentes de luz: los diodos LED (*Light Emitting Diodes*) y los diodos ILD (*Injection Laser Diode*). Ambos son dispositivos semiconductores que emiten un haz de luz cuando se les aplica una tensión. El LED es menos costoso, opera en un rango mayor de temperaturas y tiene un tiempo de vida media superior. El ILD, cuyo funcionamiento está basado en el mismo principio que los láser, es más eficaz y puede proporcionar velocidades de transmisión superiores.

Existe una relación entre la longitud de onda utilizada, el tipo de transmisión y la velocidad de transmisión que se puede conseguir. Tanto en monomodo como en multimodo se pueden admitir diferentes longitudes de onda, pudiéndose utilizar como fuentes tanto láser como diodos LED. En las fibras ópticas, debido a las características de la atenuación del medio y por las propiedades de las fuentes y receptores, la luz se propaga en cuatro regiones o «ventanas» mostradas en la Tabla 4.5.

Nótese el tremendo ancho de banda disponible. Para las cuatro ventanas, los anchos de banda son 33 THz, 12 THz, 4 THz y 7 THz, lo que corresponde a varios órdenes de magnitud más que el ancho de banda disponible en el espectro de radio-frecuencia.

Tabla 4.5. Rangos de frecuencia para varias fibras ópticas.

Rango de longitudes de onda (en el vacío) (nm)	Rango de frecuencia (THz)	Etiqueta	Tipo de fibra	Aplicación
820 a 900	366 a 33		Multimodo	LAN
1.280 a 1.350	234 a 222	S	Monomodo	Varias
1.528 a 1.561	196 a 192	C	Monomodo	WDM
1.561 a 1.620	192 a 185	L	Monomodo	WDM

WDM = Multiplexación por división en frecuencias (*Wavelength Division Multiplexing, véase* Capítulo 8).

Un posible aspecto confuso de las cifras que se dan para la transmisión con fibras ópticas es que, siempre, las prestaciones de la fibra se facilitan en términos de longitud de onda en lugar de en frecuencias. Las longitudes de onda que aparecen en gráficas y tablas corresponden a transmisión en el vacío. Sin embargo, en la fibra la velocidad de propagación es siempre inferior a la velocidad de la luz en el vacío (c), consecuentemente, aunque la frecuencia de la señal no cambia, la longitud de onda sí.

Ejemplo 4.1. Para una longitud de onda en el vacío de 1.550 nm, la frecuencia correspondiente es $f = c/\lambda = (3 \times 10^8)/(1.550 \times 10^{-9}) = 193{,}4 \times 10^2 = 193{,}4$ THz. En una fibra monomodo convencional, la velocidad de propagación es aproximadamente $v = 2{,}04 \times 10^8$. En este caso, una frecuencia de 193,4 THz corresponde a una longitud de onda de $\lambda = v/f = = (2{,}04 \times 10^8)/(193{,}4 \times 10^{12}) = 1.055$ nm. Por tanto, en esta fibra, cuando se mencione una longitud de onda de 1.550 nm, en realidad la longitud de onda real es 1.055 nm.

Las cuatro ventanas de transmisión están en la zona infrarroja del espectro de frecuencias, por debajo del espectro visible que está situado entre los 400 y 700 nm. Las pérdidas son menores cuanto mayores sean las longitudes de onda, permitiendo así mayores velocidades de transmisión sobre distancias superiores. En la actualidad, la mayoría de las aplicaciones usan como fuentes diodos LED a 850 nm. Aunque esta elección es relativamente barata, su uso está generalmente limitado a velocidades de transmisión por debajo de 100 Mbps y a distancias de pocos kilómetros. Para conseguir mayores velocidades de transmisión y mayores distancias es necesario transmitir con un LED o un láser a 1.300 nm y, si todavía se necesitan mejores prestaciones, entonces hay que recurrir al uso de emisores láser a 1.500 nm.

En la Figura 4.3c se muestra la atenuación en función de la longitud de onda para una fibra óptica convencional. La forma irregular de la curva se debe a los distintos factores que contribuyen a la atenuación. Los dos más importantes son la absorción y la dispersión (*scattering*). En este contexto, *la dispersión* se refiere al cambio de dirección que sufren los rayos de luz al chocar con pequeñas partículas o impurezas del medio.

4.2. TRANSMISIÓN INALÁMBRICA

En el estudio de las comunicaciones inalámbricas se van a considerar tres intervalos de frecuencias. El primer intervalo definido, desde 1 GHz (Gigahercio = 10^9 Hercios) hasta 40 GHz, se denomina de **frecuencias microondas**. En estas frecuencias de trabajo se pueden conseguir haces altamente direccionales, por lo que las microondas son adecuadas para enlaces punto a punto. Las microondas también se usan en las comunicaciones satelitales. Las frecuencias que van desde 30 MHz a 1 GHz son adecuadas para las aplicaciones omnidireccionales. A este rango de frecuencias lo denominaremos intervalo de **ondas de radio**.

Otro intervalo importante de frecuencias, para aplicaciones de cobertura local, es la zona infrarroja del espectro, definida aproximadamente por el rango de frecuencias comprendido entre 3×10^{11} y 2×10^{14} Hz. Los infrarrojos son útiles para las conexiones locales punto a punto, así como para aplicaciones multipunto dentro de áreas confinadas, por ejemplo dentro de una habitación.

En los medios no guiados, la transmisión y la recepción se realiza mediante una antena. Antes de estudiar los distintos tipos de transmisiones inalámbricas, a continuación se proporciona una breve introducción a las antenas.

ANTENAS

Una antena se puede definir como un conductor eléctrico (o un conjunto de conductores) utilizado para radiar o captar energía electromagnética. Para transmitir la señal, la energía eléctrica proveniente del transmisor se convierte a energía electromagnética en la antena, radiándose al entorno cercano (la atmósfera, el espacio o el agua). Para recibir una señal, la energía electromagnética capturada por la antena se convierte a energía eléctrica y se pasa al receptor.

En las comunicaciones bidireccionales, la misma antena se puede usar y, a menudo se usa, tanto para la transmisión como para la recepción. Esto es factible debido a que cualquier antena transfiere energía desde el entorno hacia el receptor con la misma eficacia con la que transfiere energía en el sentido contrario, suponiendo que se usa la misma frecuencia en ambas direcciones. En otras palabras, las características de una antena son las mismas para recibir que para transmitir energía electromagnética.

En general, una antena radiará potencia en todas las direcciones, si bien normalmente no lo hará igual de bien en todas las direcciones. Una forma habitual de caracterizar las prestaciones de una antena es mediante su diagrama de radiación, el cual consiste en una representación gráfica de las propiedades de radiación de la antena en función de la dirección. El diagrama de radiación más simple corresponde con el caso ideal, denominado la antena isotrópica. Una **antena isotrópica** es un punto en el espacio que radia potencia de igual forma en todas las direcciones. En este caso, el diagrama de radiación consistirá en una esfera centrada en la posición de la antena isotrópica.

La antena parabólica de reflexión

Un tipo muy importante de antenas son las denominadas **antenas parabólicas de reflexión**, las cuales se utilizan en aplicaciones de microondas terrestres y satelitales. Si se recuerdan conceptos de geometría básica, una parábola es el lugar geométrico de todos los puntos que equidistan de una línea recta dada y de un punto fijo que no pertenecen a la recta. El punto de referencia se denomina *foco* y la línea recta se denomina *generatriz* (*véase* Figura 4.5a). Si la parábola se hace girar en torno a su eje se genera una superficie denominada *paraboloide*. Cualquier corte o sección paralelos al eje de un paraboloide será una parábola; además, cualquier sección perpendicular al eje será un círculo. Este tipo de superficies se utilizan en faros, telescopios ópticos y radiotelescopios, así como en antenas de microondas, ya que se verifica la siguiente propiedad: las ondas reflejadas en una parábola y que provengan de cualquier fuente de energía electromagnética (o sonido) que esté situada en su foco, seguirán trayectorias paralelas al eje de la parábola. En la Figura 4.5b se muestra una sección transversal de este efecto. Teóricamente, este efecto consigue un haz paralelo sin dispersión alguna. En la práctica, habrá dispersión debido a que la fuente de energía siempre ocupará más de un punto. Cuanto mayor sea el diámetro de la antena, más direccional será el haz. En el receptor, si las ondas recibidas son paralelas al eje de la parábola reflectante, la señal resultante estará concentrada en el foco.

Ganancia de una antena

La **ganancia de una antena** es una medida de su direccionalidad. Dada una dirección, se define la ganancia de una antena como la potencia de salida, en esa dirección, comparada con la potencia transmitida en cualquier dirección por una antena omnidirecional ideal (o antena isotrópica). Por ejemplo, si una antena proporciona una ganancia de 3 dB en una dirección, esa antena mejora a la antena isotrópica en esa dirección en 3 dB, es decir, en un factor 2. El incremento de potencia radiada en una dirección dada se consigue a expensas de la potencia radiada en las otras direcciones.

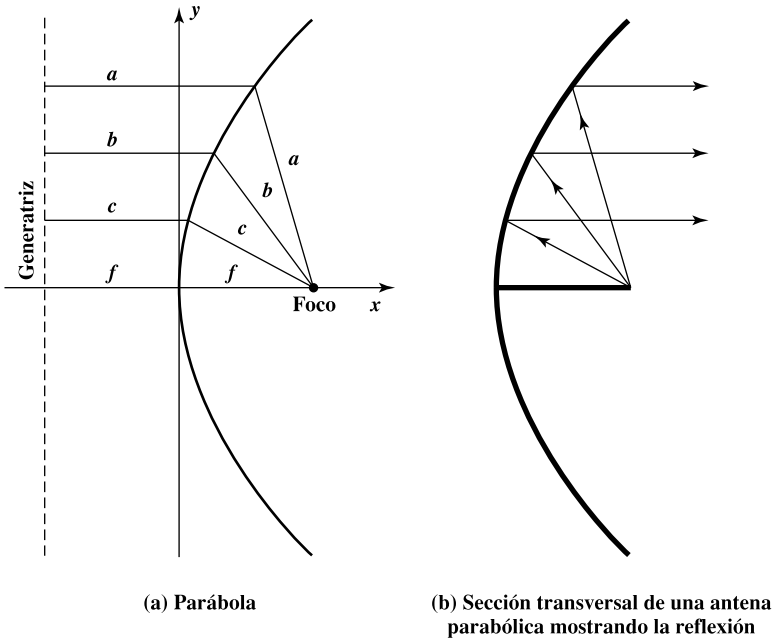


Figura 4.5. Antena parabólica de reflexión.

Es importante resaltar que la ganancia de una antena no se refiere al incremento de potencia transmitida respecto a la potencia de entrada, sino que es una medida de la direccionalidad.

Un concepto relacionado con la ganancia de una antena es el **área efectiva**. El área efectiva de una antena está relacionada con su tamaño físico y con su geometría. La relación entre la ganancia de una antena y su área efectiva viene dada por:

$$G = \frac{4\pi A_e}{\lambda^2} = \frac{4\pi f^2 A_e}{\mathrm{c}^2} \tag{4.1}$$

donde

G = ganancia de la antena.
A_e = área efectiva.
f = frecuencia de la portadora.
c = velocidad de la luz ($\approx 3 \times 10^8$ m/s).
λ = longitud de onda de la portadora.

Por ejemplo, el área efectiva de una antena isotrópica ideal es $\lambda^2/4\pi$, siendo la ganancia en potencia igual a 1; el área efectiva de una antena parabólica de área A será 0,56A, siendo la ganancia en potencia igual a $7A/\lambda^2$.

Ejemplo 4.2. Sea una antena parabólica de reflexión con un diámetro de 2 m, funcionando a una frecuencia de 12 GHz. ¿Cuál es su área efectiva y la ganancia de la antena? Se tiene que el área es $A = \pi r^2 = \pi$ y el área efectiva es $A_e = 0{,}56\pi$. La longitud de onda es $\lambda = \mathrm{c}/f = = (3 \times 10^8)/(12 \times 10^9) = 0{,}025$ m. Entonces

$$G = (7A)/\lambda^2 = (7 \times \pi)/(0{,}025)^2 = 35.186; \qquad G_{\mathrm{dB}} = 45{,}46 \text{ dB}$$

MICROONDAS TERRESTRES

Descripción física

La antena más común en las microondas es la parabólica tipo «plato». El diámetro típico es de unos 3 metros. Esta antena se fija rígidamente de forma tal que el haz debe estar perfectamente enfocado siguiendo la trayectoria visual hacia la antena receptora. Las antenas de microondas se sitúan a una altura suficientemente elevada sobre el nivel del suelo para así conseguir una separación mayor entre ellas y evitar posibles obstáculos en la transmisión. Para conseguir transmisiones a larga distancia, se concatenan distintos enlaces punto a punto entre antenas situadas en torres adyacentes, hasta cubrir la distancia deseada.

Aplicaciones

Los sistemas de microondas terrestres se usan principalmente en servicios de telecomunicación de larga distancia, como alternativa al cable coaxial o a las fibras ópticas. Para una distancia dada, las microondas requieren menor número de repetidores o amplificadores que el cable coaxial pero, por el contrario, exigen que las antenas estén perfectamente alineadas. El uso de las microondas es frecuente en la transmisión de televisión y de voz.

Otro uso cada vez más frecuente es en enlaces punto a punto a cortas distancias entre edificios. En este último caso, aplicaciones típicas son circuitos cerrados de TV o interconexiones entre redes locales. Además, las microondas a corta distancia también se utilizan en las aplicaciones denominadas *bypass*. Al usar la técnica *bypass* una determinada compañía puede establecer un enlace privado hasta el centro proveedor de transmisiones a larga distancia, evitando así tener que contratar el servicio a la compañía telefónica local.

Las microondas también se utilizan frecuentemente en los sistemas celulares, los cuales serán estudiados en el Capítulo 14.

Características de transmisión

El rango de operación de las microondas cubre una parte sustancial del espectro electromagnético. Su banda de frecuencias está comprendida entre 1 y 40 GHz. Cuanto mayor sea la frecuencia utilizada, mayor es el ancho de banda potencial y, por tanto, mayor es la posible velocidad de transmisión. En la Tabla 4.6 se indican diversos valores de anchos de banda y velocidades de transmisión de datos para algunos sistemas típicos.

Tabla 4.6. Prestaciones típicas de las microondas digitales.

Banda (GHz)	Ancho de banda (MHz)	Velocidad de transmisión (Mbps)
2	7	12
6	30	90
11	40	135
18	220	274

Al igual que en cualquier sistema de transmisión, la principal causa de pérdidas en las microondas es la atenuación. Para la microondas (y también para la banda de radiofrecuencias), la pérdida se puede expresar como

$$L = 10 \log \left(\frac{4\pi d}{\lambda} \right)^2 \text{dB} \tag{4.2}$$

donde d es la distancia y λ es la longitud de onda, expresadas en las mismas unidades. Es decir, la pérdida varía con el cuadrado de la distancia, a diferencia del cable coaxial y el par trenzado, en los que las pérdidas tienen una dependencia exponencial con la distancia (siendo lineal si se expresa en decibelios). Por tanto, en los sistemas que usan microondas, los amplificadores o repetidores pueden estar más separados entre sí (de 10 km a 100 km generalmente). La atenuación aumenta con la lluvia, siendo este efecto especialmente significativo para frecuencias por encima de 10 GHZ. Otra dificultad adicional son las interferencias. Debido a la popularidad creciente de las microondas, las áreas de cobertura se pueden solapar, haciendo que las interferencias sean siempre un peligro potencial. Así pues, la asignación de bandas tiene que realizarse siguiendo una regulación estricta.

Las bandas más usuales en la transmisión a larga distancia se sitúan entre 4 GHz y 6 GHz. Debido a la creciente congestión que están sufriendo estas bandas, últimamente se está utilizando igualmente la banda de 11 GHz. La banda de 12 GHz se usa para la distribución de TV por cable. Aquí, las microondas se utilizan para distribuir la señal de TV a las instalaciones locales de CATV. Posteriormente, las señales se distribuyen a los usuarios finales mediante cable coaxial. Las microondas a altas frecuencias se están utilizando en enlaces punto a punto entre edificios cercanos. Para tal fin, se usa generalmente la banda de 22 GHz. Las bandas de frecuencias superiores son menos útiles para distancias más largas, debido a que cada vez la atenuación es mayor; ahora bien, son bastante adecuadas para distancias más cortas. Y lo que es más, a frecuencias superiores, las antenas son más pequeñas y más baratas.

MICROONDAS POR SATÉLITE

Descripción física

Un satélite de comunicaciones es esencialmente una estación que retransmite microondas. Se usa como enlace entre dos o más receptores/transmisores terrestres, denominados estaciones base. El satélite recibe la señal en una banda de frecuencia (canal ascendente), la amplifica o repite y, posteriormente, la retransmite en otra banda de frecuencia (canal descendente). Cada uno de los satélites geoestacionarios operará en una serie de bandas de frecuencias llamadas **canales *transpondedores***, o simplemente **transpondedores (*transponders*)**.

La Figura 4.6 muestra dos configuraciones usuales en las comunicaciones vía satélite. En la primera de ellas, el satélite se utiliza para proporcionar un enlace punto a punto entre dos antenas terrestres alejadas entre sí. En la segunda, el satélite se usa para conectar una estación base transmisora con un conjunto de receptores terrestres.

Para que un satélite de comunicaciones funcione con eficacia, generalmente se exige que se mantenga en una órbita geoestacionaria, es decir, que mantenga su posición respecto de la tierra. Si no fuera así, no estaría constantemente alineado con las estaciones base. El satélite, para mantenerse geoestacionario, debe tener un periodo de rotación igual al de la tierra y esto sólo ocurre a una distancia aproximada de 35.863 km sobre el Ecuador.

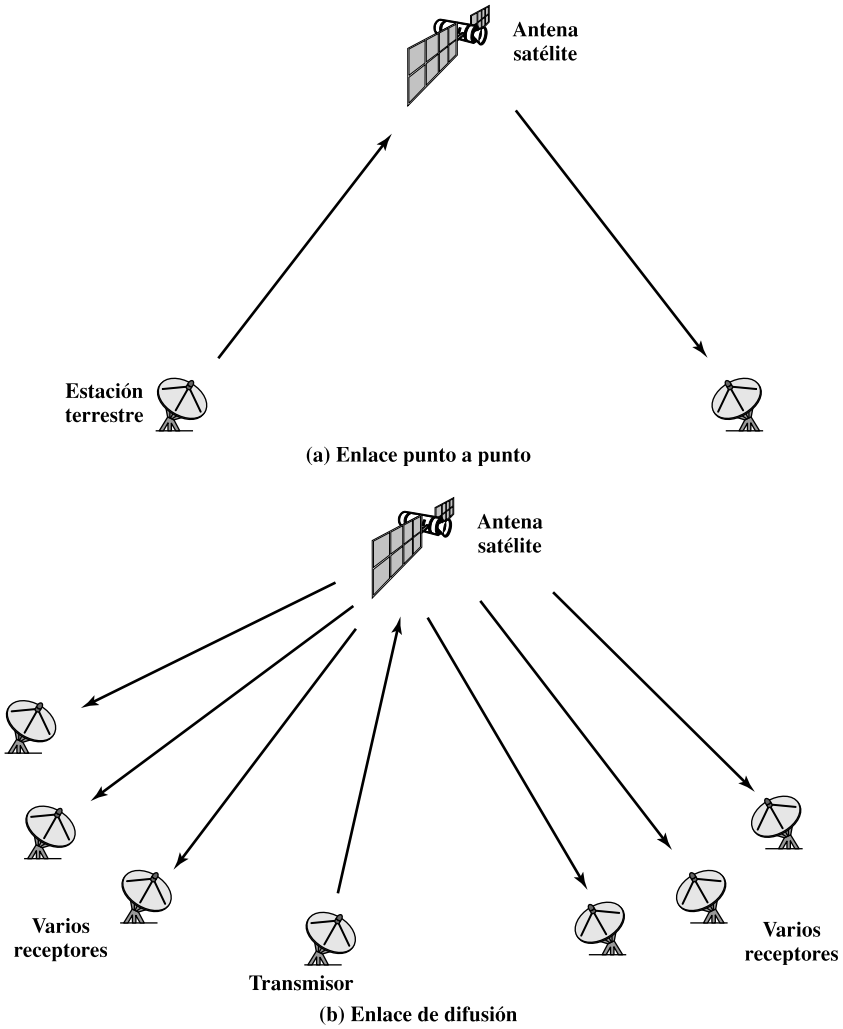


Figura 4.6. Configuraciones de comunicaciones satelitales.

Si dos satélites utilizaran la misma banda de frecuencias y estuvieran suficientemente próximos podrían interferirse mutuamente. Para evitar esto, los estándares actuales exigen una separación mínima de 4º (desplazamiento angular medido desde la superficie terrestre) en la banda 4/6 GHz, o una separación de al menos 3º en la banda de 12/14 GHz. Por tanto, el número máximo de posibles satélites está bastante limitado.

Aplicaciones

Las comunicaciones satelitales han sido una revolución tecnológica de igual magnitud que la desencadenada por la fibra óptica. Entre las aplicaciones más importantes de los satélites cabe destacar:

- La difusión de televisión.
- La transmisión telefónica a larga distancia.
- Las redes privadas.

Debido a que los satélites son de multidifusión por naturaleza, su utilización es muy adecuada para la distribución de TV, por lo que están siendo ampliamente utilizados, tanto en los Estados Unidos como en el resto del mundo. Tradicionalmente, en la distribución de TV una emisora local proporciona la programación a toda la red. Para ello, los programas se transmiten al satélite, que es el encargado de difundirlo a toda una serie de estaciones receptoras, las cuales redistribuyen la programación a los usuarios finales. La PBS (*Public Broadcasting Service*) es una red que distribuye su programación casi exclusivamente mediante el uso de canales vía satélite. Otras redes comerciales también utilizan el satélite como parte esencial de su sistema y, de igual manera, los sistemas de distribución de la TV por cable utilizan, cada vez más, el satélite como medio para obtener su programación. La aplicación más reciente de la tecnología del satélite a la televisión es la denominada difusión directa vía satélite (DBS, *Direct Broadcast Satellite*), en la que la señal de vídeo se transmite directamente desde el satélite a los domicilios de los usuarios. La disminución, tanto en coste como en tamaño, de las antenas receptoras ha hecho que esta tecnología sea factible económicamente, con lo que el número de canales disponibles es cada vez mayor.

En las redes públicas de telefonía, la transmisión vía satélite se utiliza también para proporcionar enlaces punto a punto entre las centrales. Es el medio óptimo para los enlaces internacionales que tengan un alto grado de utilización. Además, las comunicaciones satelitales son competitivas comparadas con los sistemas terrestres en gran parte de los enlaces internacionales de larga distancia.

Finalmente, la tecnología vía satélite puede facilitar un elevado número de aplicaciones de gran interés comercial. El suministrador del servicio de transmisión vía satélite puede dividir la capacidad total disponible en una serie de canales, alquilando su uso a terceras compañías. Dichas compañías, equipadas con una serie de antenas distribuidas en diferentes localizaciones, pueden utilizar un canal del satélite para establecer una red privada. Tradicionalmente, tales aplicaciones eran bastante caras, estando limitado su uso a grandes empresas. Recientemente se ha desarrollado una alternativa de bajo coste: el sistema de terminales de pequeña abertura (VSAT, *Very Small Aperture Terminal*). En la Figura 4.7 se muestra una configuración VSAT típica, consistente en una serie de estaciones equipadas con una antena VSAT de bajo coste. Mediante el uso de algún procedimiento

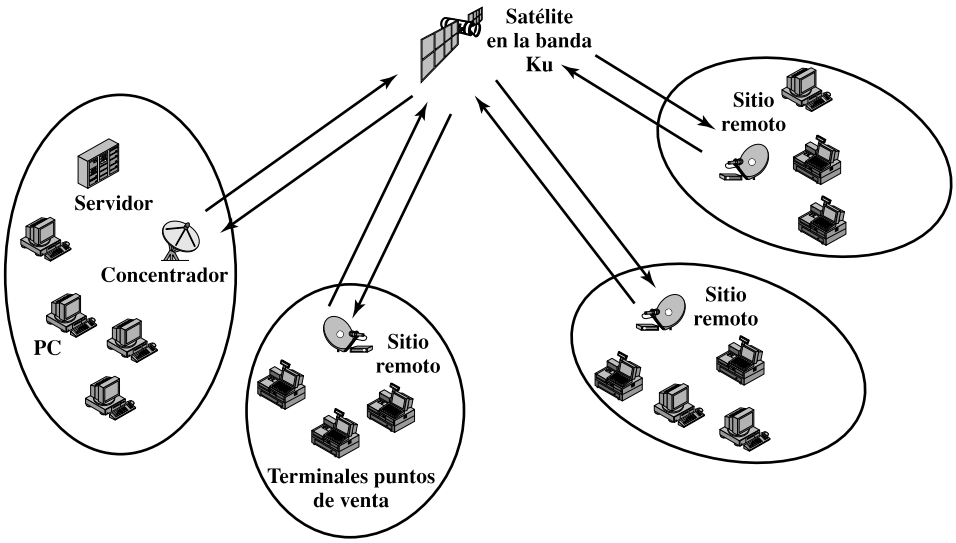


Figura 4.7. Configuración VSAT típica.

regulador, estas estaciones compartirán la capacidad del canal del satélite para transmitir a la estación central, o concentrador. Esta estación puede intercambiar información con cada uno de los abonados y puede, a su vez, retransmitir los mensajes a otras estaciones.

Características de transmisión

El rango de frecuencias óptimo para la transmisión vía satélite está en el intervalo comprendido entre 1 y 10 GHz. Por debajo de 1 GHZ, el ruido producido por causas naturales es apreciable, incluyendo el ruido galáctico, el solar, el atmosférico y el producido por interferencias con otros dispositivos electrónicos. Por encima de los 10 GHz, la señal se ve severamente afectada por la absorción atmosférica y por las precipitaciones.

La mayoría de los satélites que proporcionan servicio de enlace punto a punto operan en el intervalo entre 5,925 y 6,425 GHz para la transmisión desde las estaciones terrestres hacia el satélite (canal ascendente) y entre 3,7 y 4,2 GHz para la transmisión desde el satélite hasta la Tierra (canal descendente). Este intervalo de frecuencias se conoce como la banda 4/6 GHz. Nótese que las frecuencias ascendentes son diferentes de las descendentes. En una transmisión continua y sin interferencias, el satélite no puede transmitir y recibir en el mismo rango de frecuencias. Así pues, las señales que se reciben desde las estaciones terrestres en una frecuencia dada se deberán devolver en otra distinta.

La banda 4/6 GHz está dentro de la zona óptima de frecuencias (de 1 a 10 GHz); ahora bien, su utilización exhaustiva la ha llevado a la saturación. Debido a posibles interferencias (por ejemplo, con microondas terrestres operando en ese mismo rango), las restantes frecuencias del intervalo óptimo no se pueden utilizar. Este hecho ha motivado que se hayan asignado otras bandas alternativas como la 12/14 GHz (el canal ascendente está situado entre 14 y 14,5 GHz y el descendente está entre 11,7 a 12,2 GHz). En esta banda aparecen problemas de atenuación que se deben solventar. No obstante, se pueden usar receptores terrestres más baratos y de dimensiones más reducidas. Se ha pronosticado que esta banda también se saturará, por lo que se está proyectando la utilización de la banda 20/30 GHz (enlace ascendente: desde 27,5 a 30,0 GHz; enlace descendente: de 17,7 a 20,2 GHz). En esta banda la atenuación es incluso superior, ahora bien, por el contrario proporcionará un ancho de banda mayor (2.500 MHz comparados con los 500 MHz anteriores), a la vez que los receptores podrán ser todavía más pequeños y económicos.

Es interesante comentar algunas de las propiedades peculiares de las comunicaciones vía satélite. En primer lugar, debido a las grandes distancias involucradas, el retardo de propagación es aproximadamente del orden de un cuarto de segundo para una transmisión que vaya desde una estación terrestre hasta otra y que pase por el satélite. Este retardo es apreciable si se trata de una conversación telefónica ordinaria. Además, estos retrasos introducen problemas adicionales a la hora de controlar los errores y el flujo en la transmisión. Estos problemas se estudian en capítulos posteriores. En segundo lugar, los satélites con microondas son intrínsecamente un medio idóneo para las aplicaciones multidestino, es decir, aplicaciones en las que varias estaciones necesiten transmitir hacia el satélite e, igualmente, varias estaciones necesiten recibir la señal transmitida por el satélite.

ONDAS DE RADIO

Descripción física

La diferencia más apreciable entre las microondas y las ondas de radio es que estas últimas son omnidireccionales, mientras que las primeras tienen un diagrama de radiación mucho más direccio-

nal. Este hecho hace que las ondas de radio no necesiten antenas parabólicas ni necesitan que dichas antenas estén instaladas sobre una plataforma rígida para estar alineadas.

Aplicaciones

Con el término **radio** se alude de una manera poco precisa a toda la banda de frecuencias comprendida entre 3 kHz y 300 GHz. Aquí, de una manera informal, se está utilizando el término **ondas de radio** para aludir a la banda VHF y parte de UHF: de 30 MHz a 1 GHz. Este rango abarca a la radio comercial FM así como a la televisión UHF y VHF. Este intervalo también se utiliza para ciertas aplicaciones de redes de datos.

Características de transmisión

El rango de frecuencias comprendido entre 30 MHz y 1GHz es muy adecuado para la difusión simultánea a varios destinos. A diferencia de las ondas electromagnéticas con frecuencias menores, la ionosfera es transparente para las ondas con frecuencias superiores a 30 MHz. Así pues, la transmisión es sólo posible cuando las antenas estén alineadas. En esa banda no se producirán interferencias entre los transmisores debidas a las reflexiones en la atmósfera. A diferencia de la región de las microondas, las ondas de radio son menos sensibles a la atenuación producida por la lluvia.

Como en el caso de las microondas, la cantidad de atenuación debida a la distancia verifica la Ecuación (4.2); es decir, $10\log\left(\frac{4\pi d}{\lambda}\right)^2$. Debido a que tienen una longitud de onda mayor, las ondas de radio sufren, en términos relativos, una atenuación menor.

Un factor muy relevante en las ondas de radio son las interferencias por multitrayectorias. Entre las antenas, debido a la reflexión en la superficie terrestre, el mar u otros objetos, pueden aparecer multitrayectorias. Este efecto aparece con frecuencia en los receptores de TV y consiste en la aparición de varias imágenes (o sombras) producidas, por ejemplo, cuando pasa un avión por el espacio aéreo cercano.

INFRARROJOS

Las comunicaciones mediante infrarrojos se llevan a cabo mediante transmisores/receptores (transceptores, *transceivers*) que modulan luz infrarroja no coherente. Los transceptores deben estar alineados directamente, o bien deben estar accesibles a través de la reflexión en una superficie, como por ejemplo el techo de la habitación.

Una diferencia significativa entre los rayos infrarrojos y las microondas es que los primeros no pueden atravesar las paredes. Por tanto, los problemas de seguridad y de interferencias que aparecen en las microondas no se presentan en este medio de transmisión. Es más, no hay problemas de asignación de frecuencias ya que para operar en esta banda no se necesitan permisos.

4.3. PROPAGACIÓN INALÁMBRICA

Toda señal radiada por una antena puede seguir tres posibles trayectorias: la superficial, la aérea o la trayectoria visual (LOS, *Line of Sight*). La Tabla 4.7 muestra el intervalo de frecuencias

Tabla 4.7. Bandas de frecuencias.

Banda	Rango de frecuencias	Rango de longitudes de onda en el espacio libre	Características de propagación	Uso típico
Frecuencias extremadamente bajas (ELF, *Extremely Low Frequency*)	30 a 300 Hz	10.000 a 1.000 km	GW	Líneas de potencia; se utilizan en algunos sistemas de control domésticos
Frecuencias de voz (VF, *Voice Frequency*)	300 a 3.000 Hz	1.000 a 100 km	GW	Se usan en los bucles de abonado de los sistemas de telefonía
Frecuencias muy bajas (VLF, *Very Low Frequency*)	3 a 30 kHz	100 a 10 km	GW con baja atenuación diurna y nocturna; alto nivel de ruido atmosférico	Navegación en alta mar; comunicaciones submarinas
Frecuencias bajas (LF, *Low Frequency*)	30 a 300 kHz	10 a 1 km	GW; ligeramente menos fiable que VLF; absorción diurna	Navegación en alta mar; radiolocalización para comunicaciones marinas
Frecuencias medias (MF, *Medium Frequency*)	300 a 3.000 kHz	1.000 a 100 m	GW y SW nocturna; baja atenuación nocturna, siendo alta la diurna; ruido atmosférico	Radio marítima; búsqueda de direcciones; radiodifusión AM
Frecuencias altas (HF, *High Frequency*)	3 a 30 MHz	100 a 10 m	SW; la calidad varía a lo largo del día, con las estaciones y la frecuencia	Radioaficionados; radiodifusión internacional; comunicaciones militares; navegación aérea de larga distancia y comunicaciones marítimas
Frecuencias muy altas (VHF, *Very High Frequency*)	30 a 300 MHz	10 a 1 m	LOS; dispersión (*scattering*) debido a la inversión de temperaturas; ruido cósmico	Televisión VHF; radiodifusión FM, comunicaciones AM en aviones; ayudas a la navegación de aviones
Frecuencias ultra altas (UHF, *Ultra High Frequency*)	300 a 3.000 MHz	100 a 10 cm	LOS; ruido cósmico	Televisión UHF; telefonía celular; radar; enlaces de microondas; sistemas de comunicación personal
Frecuencias super altas (SHF, *Super High Frequency*)	3 a 30 GHz	10 a 1 cm	LOS; la lluvia atenúa por encima de 10 GHz; atenuación atmosférica debido al vapor de agua y al oxígeno	Comunicaciones satelitales; radar; enlaces de microondas terrestres; bucles locales inalámbricos
Frecuencias extremadamente altas (EHF, *Extremely High Frequency*)	30 a 300 GHz	10 a 1 mm	LOS; atenuación atmosférica debido al vapor de agua y al oxígeno	Experimental; bucles locales inalámbricos
Infrarrojos	300 GHz a 400 THz	1 a 770 nm	LOS	LAN infrarrojas; aplicaciones de electrónica de consumo
Luz visible	400 a 900 THz	700 a 330 nm	LOS	Comunicaciones ópticas

predominante para cada modo de los anteriores. Este texto se centrará casi exclusivamente en las comunicaciones que usen LOS; no obstante, en esta sección se proporciona un breve resumen de cada uno de los tres modos.

PROPAGACIÓN SUPERFICIAL DE ONDAS

La propagación superficial (GW, *Ground Wave*) (*véase* Figura 4.8a) sigue, con más o menos precisión, el contorno de la superficie terrestre, pudiendo alcanzar grandes distancias, más allá de la

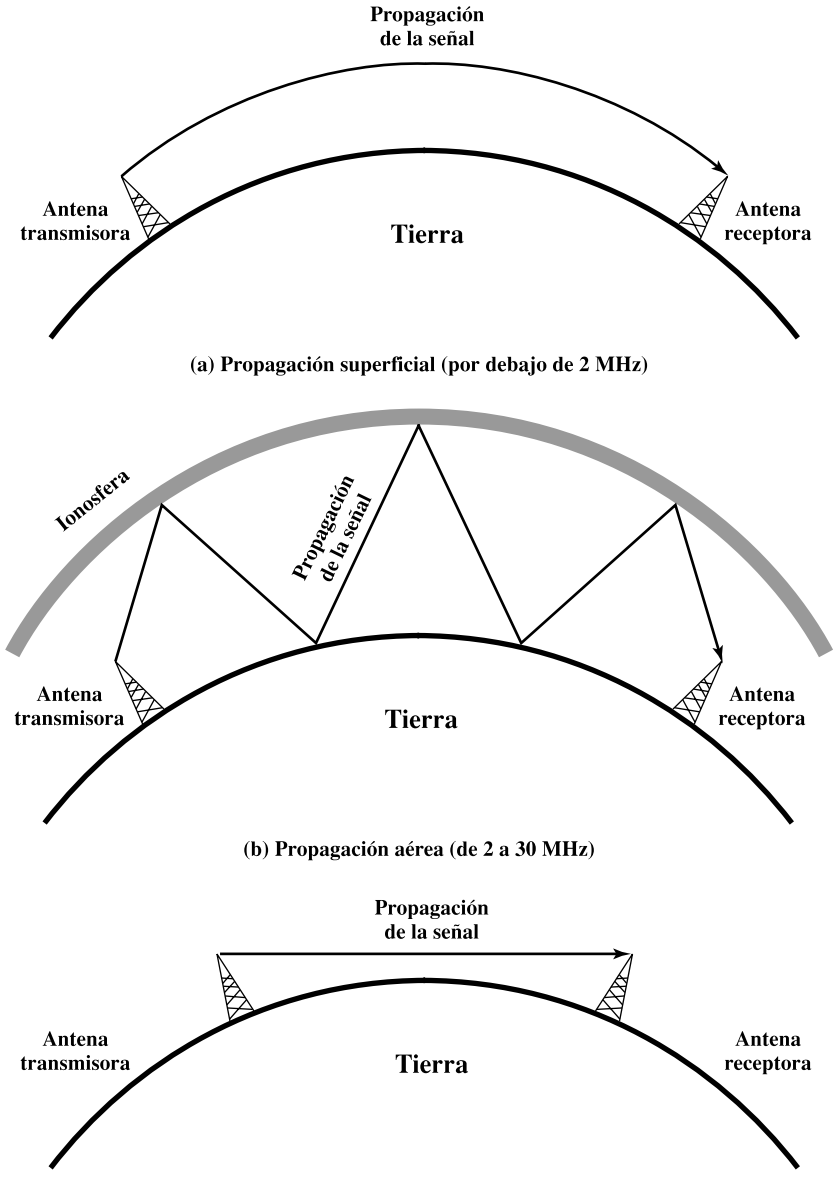


Figura 4.8. Modos de propagación inalámbricos.

línea del horizonte visual. Este efecto se da para frecuencias de hasta 2 MHz. Hay varios factores que justifican la tendencia que tienen las ondas electromagnéticas con estas frecuencias a seguir la curvatura terrestre. El primer factor es que la onda electromagnética induce una corriente en la superficie terrestre que frena al frente de onda cerca de la superficie, haciendo que éste se curve hacia abajo, adaptándose así a la curvatura de la superficie terrestre. Otro de los factores es la difracción, la cual es un fenómeno que tiene que ver con el comportamiento de las ondas electromagnéticas en presencia de obstáculos.

Las ondas electromagnéticas a estas frecuencias son dispersadas por la atmósfera, de forma tal que no llegan a penetrar en las capas altas.

El ejemplo más conocido de propagación terrestre es la radio AM.

PROPAGACIÓN AÉREA DE ONDAS

La propagación aérea de ondas (SW, *Sky Wave*) se utiliza por los radio-aficionados (*amateur radio* o *CB radio*, en inglés) y en las emisiones internacionales de radio comercial, como la BBC o la «Voice of America». En este tipo de propagación, la señal proveniente de la antena terrestre se refleja en la capa ionizada de la atmósfera alta (la ionosfera), volviendo así hacia la tierra. Aunque así dicho pareciera que la onda se refleja en la ionosfera, como si se tratara de una superficie reflectante, el efecto, en realidad, es refractario. A continuación, se explica en qué consiste la refracción.

Una señal que se propague de esta manera se desplazará dando una serie de saltos, entre la ionosfera y la superficie terrestre (*véase* Figura 4.8a). Utilizando este modo de transmisión se puede conseguir que la onda se reciba a miles de kilómetros del transmisor.

PROPAGACIÓN EN LA TRAYECTORIA VISUAL

Por encima de 30 MHz, los modos de propagación superficial o aérea no funcionan, por lo que las comunicaciones han de realizarse siguiendo la línea de visión (LOS, *Line-of-Sight*) (*véase* Figura 4.8c). En las comunicaciones vía satélite, las señales por encima de 30 MHz no se reflejan en la ionosfera, por lo que para esas frecuencias no es posible transmitir entre estaciones terrestres y satélites que estén por debajo de la línea del horizonte. En comunicaciones superficiales, para este modo de transmisión, la antena emisora y la receptora deben estar alineadas según la trayectoria visual *efectiva*. Se usa el término *efectiva* ya que las microondas son pandeadas o refractadas por la atmósfera. La cantidad de pandeo, e incluso la dirección seguida, dependerá de las condiciones, aunque, por lo general, las microondas siguen la curvatura de la tierra, por lo que llegarán más lejos que si siguieran la línea de visión óptica.

Refracción

Antes de seguir adelante, en esta sección se proporciona un breve repaso a la refracción. La refracción se produce debido a que la velocidad de las ondas electromagnéticas es una función de la densidad del medio atravesado. En el vacío, una onda electromagnética (por ejemplo la luz o una onda de radio) se propaga aproximadamente a 3×10^8 m/s. Ésta es la constante c, denominada velocidad de la luz, aunque en realidad se está refiriendo a la velocidad de la luz en el vacío[2]. En

[2] El valor exacto es 299.792.458 m/s.

el aire, agua, cristal o cualquier otro medio transparente, o parcialmente transparente, las ondas electromagnéticas viajan a velocidades menores que c.

Cuando una onda electromagnética pasa de un medio con una densidad a otro con densidad distinta, su velocidad cambia. El efecto de esto es desviar la dirección de la onda en la separación entre los dos medios. Al pasar de un medio menos denso a otro con densidad mayor, la onda se desviará hacia el medio más denso. Este fenómeno se puede observar sumergiendo parcialmente un palo en agua.

El **índice de refracción** de un medio respecto a otro es igual al seno del ángulo de incidencia dividido entre el seno del ángulo de refracción. El índice de refracción es también igual al cociente entre las velocidades respectivas en los dos medios. El índice absoluto de refracción de un medio se calcula en comparación con el del vacío. El índice de refracción varía con la longitud de onda, de forma tal que la refracción sufrida por señales con distintas longitudes de onda será diferente.

Aunque en una separación discreta entre dos medios la desviación de la onda será abrupta y de una vez, si se trata de una separación continua, en la que el índice de refracción varíe gradualmente, la onda se desviará gradualmente. Bajo condiciones normales de propagación, el índice de refracción de la atmósfera disminuye con la altura, por lo que las ondas de radio viajan más lentamente cerca de la tierra que a alturas mayores. Como consecuencia, se tiene que las ondas de radio se desvían suavemente hacia la tierra.

Línea de visión óptica y de radio

Si no hay obstáculos, la línea de visión óptica se puede expresar cómo:

$$d = 3{,}57\sqrt{h}$$

donde d es la distancia entre la antena y el horizonte en kilómetros y h es la altura de la antena en metros. La línea de visión efectiva, o de radio, se expresa como (*véase* Figura 4.9)

$$d = 3{,}57\sqrt{Kh}$$

donde K es un factor de ajuste que tiene en cuenta la refracción. Una buena aproximación es $K = 4/3$. Así, la distancia máxima entre dos antenas siguiendo propagación LOS es

$$3{,}57(\sqrt{Kh_1} + \sqrt{Kh_2})$$

donde h_1 y h_2 son respectivamente las alturas de las antenas.

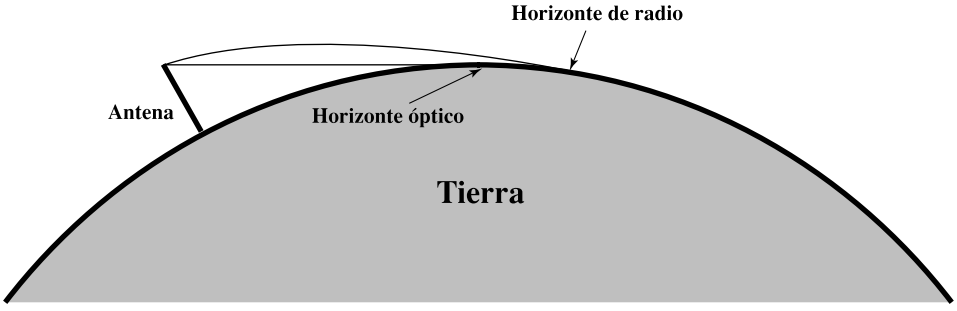


Figura 4.9. Horizonte óptico y de radio.

Ejemplo 4.3. La distancia máxima entre dos antenas para transmisión LOS, a una altura de 100 m y la otra situada a nivel de la superficie, es

$$d = 3{,}57\sqrt{Kh} = 3{,}57\sqrt{133} = 41 \text{ km}$$

Ahora, supóngase que la antena receptora está a una altura de 10 m. Para conseguir la misma distancia, ¿a qué altura debería estar la antena transmisora?

$$41 = 3{,}57(\sqrt{Kh_1} + \sqrt{13{,}3})$$

$$\sqrt{Kh_1} = \frac{41}{3{,}57} - \sqrt{13{,}3} = 7{,}84$$

$$h_1 = \frac{7{,}84^2}{1{,}33} = 46{,}2 \text{ m}$$

Esto implica un ahorro de 50 m en la altura de la antena emisora. Este ejemplo pone de manifiesto las ventajas que se pueden conseguir al elevar la antena receptora sobre la superficie, ya que se reduce la altura de la antena emisora.

4.4. TRANSMISIÓN EN LA TRAYECTORIA VISUAL

En la Sección 3.3 se han estudiado algunas de las dificultades habituales tanto en las transmisiones guiadas como en las inalámbricas. En esta sección ampliaremos el estudio para considerar algunas dificultades específicas de la transmisión inalámbrica siguiendo la trayectoria visual.

PÉRDIDA EN EL ESPACIO LIBRE

En cualquier tipo de comunicación inalámbrica la señal se dispersa con la distancia. Por tanto, una antena dada con un superficie fija recibirá menos potencia cuanto más alejada esté de la antena emisora. En comunicaciones vía satélite ésta es la principal causa de las pérdidas. Incluso en el caso de que se suponga que no hay otros fenómenos de atenuación o impedimentos, una señal transmitida se atenúa con la distancia debido a que la señal ocupa un área cada vez mayor. Este tipo de atenuación se denomina **pérdida en el espacio libre**, la cual se puede expresar en términos del cociente entre la potencia radiada, P_t y la potencia recibida en la antena, P_r, o también en decibelios, multiplicando por 10 el logaritmo del cociente. Para la antena isotrópica ideal, la pérdida en el espacio libre es

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f d)^2}{c^2}$$

donde

P_t = potencia de la señal en la antena emisora.
P_r = potencia de la señal en la antena receptora.
λ = longitud de onda de la portadora.
d = longitud o separación entre las antenas.
c = velocidad de la luz (3×10^8 m/s).

Donde d y λ están expresadas en la misma unidad (por ejemplo en metros). Se puede reescribir como

$$L_{\text{dB}} = 10\log\frac{P_t}{P_r} = 20\log\sqrt{\frac{4\pi d}{\lambda}} = -20\log(\lambda) + 20\log(d) + 21{,}98 \text{ dB}$$
$$= 20\log\sqrt{\frac{4\pi f d}{\text{c}}} = 20\log(f) + 20\log(d) - 147{,}56 \text{ dB} \tag{4.3}$$

En la Figura 4.10 se representa la ecuación[3] de la pérdida en el espacio libre.

Para otro tipo de antenas, se ha de tener en cuenta la ganancia de la misma, la cual verifica la ecuación de la pérdida en el espacio libre:

$$\frac{P_t}{P_r} = \frac{(4\pi)^2(d)^2}{G_r G_t \lambda^2} = \frac{(\lambda d)^2}{A_r A_t} = \frac{(\text{c}d)^2}{f^2 A_r A_t}$$

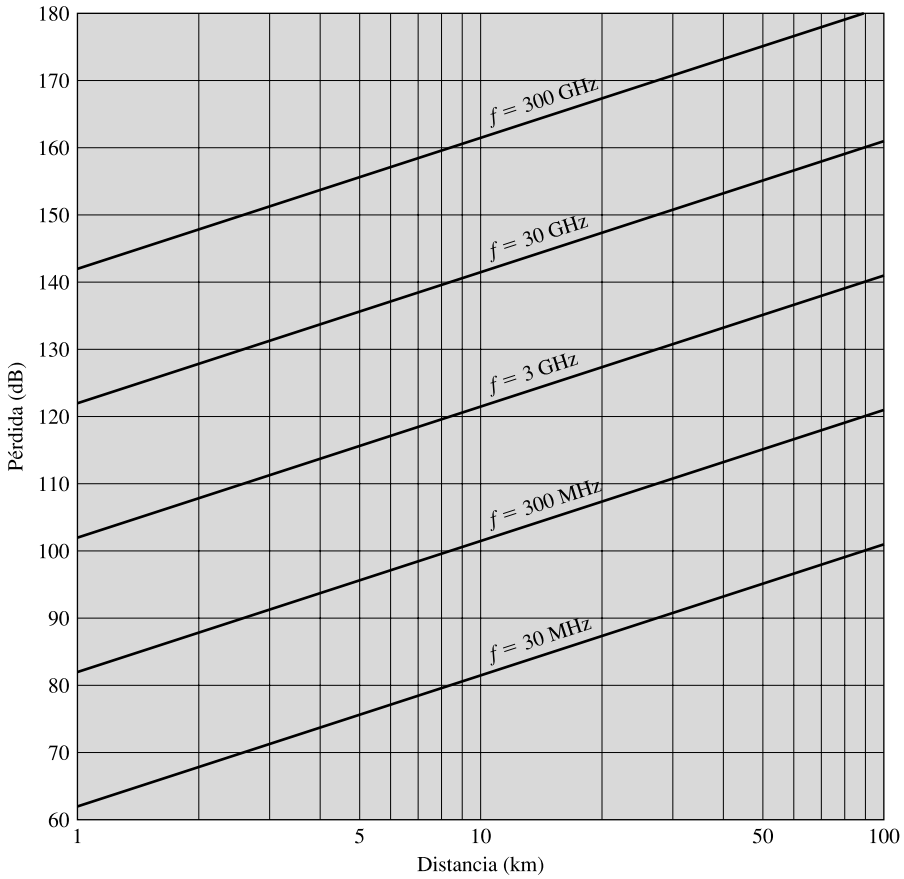


Figura 4.10. Pérdida en el espacio libre.

[3] Como se menciona en el Apéndice 3A, en la bibliografía hay algunas inconsistencias en el uso de los términos ganancia y pérdida. La Ecuación (4.3) sigue la convención de la Ecuación (2.2).

donde

G_t = ganancia de la antena emisora.

G_r = ganancia de la antena receptora.

A_t = área efectiva de la antena emisora.

A_r = área efectiva de la antena receptora.

El cociente de la tercera igualdad anterior se ha obtenido usando la relación entre la ganancia de una antena y el área efectiva, Ecuación (4.1). Se puede rescribir la ecuación de la pérdida como

$$\begin{aligned} L_{\text{dB}} &= 20\log(\lambda) + 20\log(d) - 10\log(A_tA_r) \\ &= -20\log(f) + 20\log(d) - 10\log(A_tA_r) + 169{,}54 \text{ dB} \end{aligned} \tag{4.4}$$

Por tanto, para antenas con las mismas dimensiones e igualmente separadas, cuanto mayor es la longitud de onda de la portadora (es decir, cuanto menor es la frecuencia de la portadora f) mayor es la pérdida en el espacio libre. Es interesante comparar la Ecuación (4.3) con la Ecuación (4.4). La Ecuación (4.3) indica que, al aumentar la frecuencia, la pérdida en el espacio libre también aumenta; esto puede indicar que a altas frecuencias, las pérdidas pueden llegar a ser intolerables. Sin embargo, la Ecuación (4.4) muestra que esto (el incremento en la pérdida) se puede compensar fácilmente aumentando las ganancias de las antenas. De hecho, hay una ganancia neta al aumentar la frecuencia, manteniendo los otros factores constantes. La Ecuación (4.3) muestra que, para una distancia fija, un incremento en frecuencias implica un incremento en la pérdida medida en un factor igual a $20\log(f)$. No obstante, si se tiene en cuenta la ganancia de la antena, para una antena con un área fija, entonces el cambio en la pérdida viene dado por $-20\log(f)$; es decir, realmente hay una disminución de la pérdida al aumentar la frecuencia.

Ejemplo 4.4. Calcular la pérdida en el espacio libre de una antena isotrópica a 4 GHz para el camino más corto a un satélite geoestacionario (35.863 km). A 4 GHz, la longitud de onda es $(3 \times 10^8)/(4 \times 10^9) = 0{,}075$ m. Entonces,

$$L_{\text{dB}} = -20\log(0{,}075) + 20\log(35{,}853 \times 10^6) + 21{,}98 = 195{,}6 \text{ dB}$$

Ahora, considérese la ganancia de las antenas situadas en tierra y en el satélite. Valores típicos son 48 dB y 44 dB respectivamente. La pérdida en el espacio libre es

$$L_{\text{dB}} = 195{,}6 - 44 - 48 = 103{,}6 \text{ dB}$$

Si ahora se supone que la potencia transmitida es 250 W en la estación terrestre. ¿Cuál será la potencia recibida por la antena del satélite? Una potencia de 250 W se traduce en 24 dBW, por lo que la potencia recibida es $24 - 103{,}6 = -79{,}6$ dBW.

ABSORCIÓN ATMOSFÉRICA

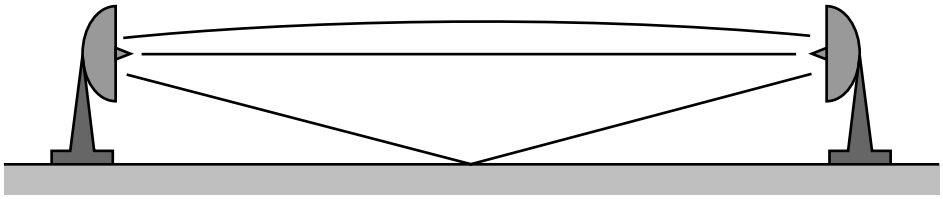
Entre la antena emisora y la receptora existe una pérdida adicional causada por la absorción atmosférica. El vapor de agua y el oxígeno son los principales causantes de esta atenuación. Hay un pico de absorción en la vecindad de los 22 GHz debido al vapor de agua. A frecuencias por debajo de 15 GHz, la atenuación es menor. La presencia de oxígeno causa un pico de absorción en torno a 60 GHz, aunque es menos apreciable por debajo de 30 GHz. La lluvia y la niebla (gotitas de agua suspendidas) hacen que las ondas de radio se dispersen (sufran *scattering*) y, en definitiva, se

atenúen. En este contexto, el término *scattering* se refiere al fenómeno que consiste en el cambio de dirección o frecuencia que sufre una onda al encontrarse con partículas de materia. Ésta puede ser la causa principal de la pérdida de la señal. Por tanto, en zonas de grandes precipitaciones, o las longitudes de los caminos a recorrer se acortan, o se deben usar bandas de frecuencias menores.

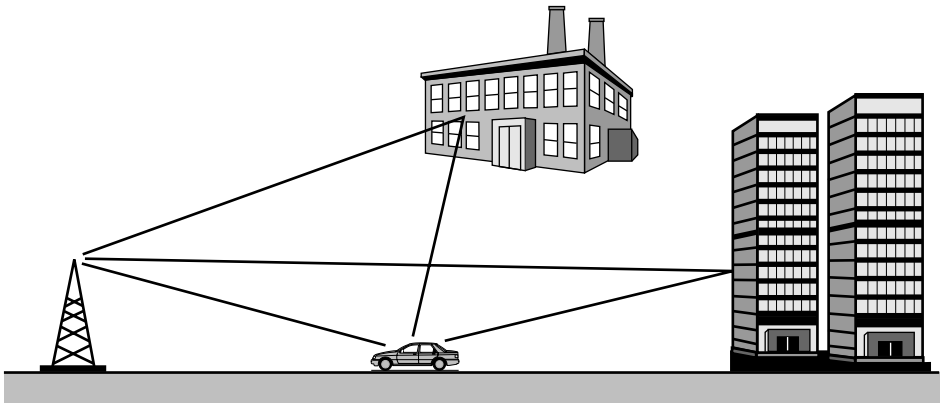
MULTITRAYECTORIAS

En aplicaciones inalámbricas, en las que hay una libertad relativa para situar las antenas, se pueden localizar de forma tal que no haya obstáculos entre ellas, así estarán perfectamente alineadas siguiendo la trayectoria visual desde la antena emisora a la receptora. Esto es lo habitual en muchas aplicaciones vía satélite y en microondas punto a punto. En otros casos, como en la telefonía móvil, hay un gran número de obstáculos. La señal se refleja en tantos obstáculos que el receptor recibirá varias versiones de la señal con retardos diferentes. De hecho, en casos extremos, no se recibirá la señal directa. Dependiendo de las diferencias entre las longitudes de las trayectorias del camino directo y los reflejados, la señal recibida total puede llegar a ser mayor o menor que la señal original. El realce o cancelación de la señal proveniente de las múltiples trayectorias se puede controlar para el caso de que las antenas estén fijas y sean bien conocidas, al igual que entre satélites y estaciones terrestres. Una excepción es el caso en el que la trayectoria pase a través de agua, ya que en ese caso habría que tener presente la superficie reflectante del agua en movimiento. En la telefonía móvil o en transmisiones entre antenas no fijas, las multitrayectorias son un problema de suma importancia.

La Figura 4.11 muestra, en términos genéricos, los distintos tipos de interferencias por multitrayectorias que se pueden dar en transmisiones superficiales usando microondas fijas o comunica-



(a) Trayectoria visual para microondas



(b) Radio móvil

Figura 4.11. Ejemplos de interferencias por multitrayectorias.

ciones móviles. En el caso de microondas con antenas inmóviles, además de la transmisión siguiendo la trayectoria visual, la señal puede seguir una trayectoria curva a través de la atmósfera debido a la refracción, pudiéndose reflejar igualmente en la superficie terrestre. En el caso de comunicaciones móviles, tanto las diversas infraestructuras como los accidentes topográficos pueden presentar superficies de reflexión.

REFRACCIÓN

Las ondas de radio se pueden refractar (o desviar) cuando se propagan a través de la atmósfera. La refracción es causada por los cambios en la velocidad de la señal al cambiar su altura o por otro tipo de cambios espaciales debido a las condiciones atmosféricas. Normalmente, la velocidad de la señal aumenta con la altura, haciendo que las ondas de radio se desvíen hacia la superficie terrestre. No obstante, en ciertas ocasiones, las condiciones metereológicas pueden implicar variaciones en la velocidad con la altura que sean significativamente distintas de las variaciones típicas esperadas. Esto puede dar lugar a que sólo una fracción, o incluso nada, de la onda transmitida siguiendo la trayectoria visual llegue a la antena receptora.

4.5. LECTURAS RECOMENDADAS Y SITIOS WEB

[FREE98] presenta una descripción detallada de las características de transmisión de los medios citados en este capítulo. En [REEV95] se realiza un excelente estudio de los pares trenzados y de las fibras ópticas. [BORE97] es un tratado completo sobre los componentes de la transmisión sobre fibra óptica. Otro artículo de calidad sobre el tema es [WILL97]. [FREE02] es una referencia técnica muy detallada sobre fibras ópticas. En [STAL00] se discuten con más detalle las características de los medios de transmisión en LAN.

Para un tratamiento más profundo de la propagación y transmisión inalámbrica, *véanse* [STAL02] y [RAPP96]. [FREE97] es una referencia técnica excelente en cuestiones inalámbricas.

BORE97 Borella, M., et al., «Optical Components for WDM Lightwave Networks». *Proceedings of the IEEE*, agosto 1997.

FREE97 Freeman, R. *Radio System Deisgn for Telecommunications*. New York: Wiley, 1997.

FREE98 Freeman, R. *Telecommunication Transmission Handbook*. New York: Wiley, 1998.

FREE02 Freeman, R. *Fiber-Optic Systems for Telecommunications*. New York: Wiley, 2002.

RAPP96 Rappaport, T. *Wireless Communications*. Upper Saddle River, NJ: Prentice Hall, 1996.

REEV95 Reeve, W. Subscriber Loop Signaling and Transmission Hanbdbook. Piscataway, NJ: IEEE Press, 1995.

STAL00 Stallings, W. *Local and Metropolitan Area Networks*, 4*th Edition*. Upper Saddle River, NJ: Prentice Hall, 2000.

STAL02 Stallings, W. *Wireless Communications and Networks*. Upper Saddle River, NJ: Prentice Hall, 2002.

WILL97 Willner, A. «Mining the Optical Bandwidth for a Terabit per Second». *IEEE Spectrum*, abril 1997.

SITIOS WEB RECOMENDADOS

- **«Simeon Company»:** una buena colección de artículos técnicos sobre cableado, además de información sobre estándares de cableado.
- **«Wireless Developer Network»:** noticias, tutoriales y discusiones sobre distintos aspectos de las comunicaciones inalámbricas.

4.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

absorción atmosférica
antena
antena direccional
antena isotrópica
antena omnidireccional
antena parabólica de reflexión
área efectiva
atenuación
cable coaxial
dispersión (*Scattering*)
fibra óptica
frecuencias de microondas
ganancia de una antena
índice de refracción
infrarrojo
trayectoria visual (LOS, *Line of Sight*)
LOS óptica
medio de transmisión
medio guiado
medio no guiado
microondas terrestres
multitrayectoria
par trenzado
par trenzado apantallado (STP, *Shielded Twisted Pair*)
par trenzado no apantallado (UTP, *Unshielded Twisted Pair*)
pérdida en el espacio libre
propagación aérea de ondas
propagación superficial de ondas
radio
radio LOS
reflexión
refracción
satélite
transmisión inalámbrica

CUESTIONES DE REPASO

4.1 ¿Por qué hay dos cables en un par trenzado de cobre?

4.2. ¿Cuáles son las limitaciones del par trenzado?

4.3. ¿Cuál es la diferencia entre el par trenzado no apantallado y el par trenzado apantallado?

4.4. Describir los principales componentes del cable de fibra óptica.

4.5. ¿Qué ventajas y desventajas tiene la transmisión de microondas?

4.6. ¿Qué es la difusión directa por satélite (DBS, *Direct Broadcast Satellite*)?

4.7. ¿Por qué un satélite debe usar frecuencias ascendentes y descendentes distintas?

4.8. Indique las diferencias más significativas entre la difusión de radio y las microondas.

4.9. ¿Qué dos funciones realiza una antena?

4.10. ¿Qué es una antena isotrópica?

4.11. ¿Cuál es la ventaja de una antena parabólica por reflexión?

4.12. ¿Qué factores determinan la ganancia de una antena?

4.13. ¿Cuál es la principal causa de la pérdida de señal en comunicaciones vía satélite?

4.14. ¿Qué es la refracción?

4.15. ¿Qué diferencia hay entre difracción y dispersión?

EJERCICIOS

4.1. Supóngase que unos datos se almacenan en disquetes de 1,4 Mbytes que pesan 30 g cada uno y que una compañía aérea transporta 10^4 kg de disquetes a una velocidad de 1.000 km/h sobre una distancia de 5.000 km. ¿Cuál es la velocidad de transmisión en bits por segundo de este sistema?

4.2. Sea una línea telefónica caracterizada por una pérdida de 20 dB. La potencia de la señal a la entrada es de 0,5 W y el nivel del ruido a la salida es de 4,5 μW. Calcule la relación señal ruido para la línea en dB.

4.3. Dada una fuente de 100 W, determine la máxima longitud alcanzable en los siguientes medios de transmisión, si la potencia a recibir es 1 vatio:

a) Un par trenzado de 0,5 mm (24 gauges) a 300 kHz.

b) Un par trenzado de 0,5 mm (24 gauges) a 1 MHz.

c) Un cable coaxial de 9,5 mm a 1 MHz.

d) Un cable coaxial de 9,5 mm a 25 MHz.

e) Una fibra óptica trabajando a su frecuencia óptima.

4.4. El cable coaxial es un sistema de transmisión con dos conductores. ¿Qué ventaja tiene conectar la malla exterior a tierra?

4.5. Demuestre que duplicando la frecuencia de transmisión o duplicando la distancia entre las antenas de transmisión y recepción, la potencia recibida se atenúa en 6 dB.

4.6. La profundidad en el océano a la que se detectan las señales electromagnéticas generadas desde aeronaves crece con la longitud de onda. Por tanto, los militares encontraron que usando longitudes de onda muy grandes, correspondientes a 30 Hz, podrían comunicarse con cualquier submarino alrededor del mundo. La longitud de las antenas es deseable que sea del orden de la mitad de la longitud de onda. ¿Cuál debería ser la longitud típica de las antenas para operar a esas frecuencias?

4.7. La potencia de la señal de voz está concentrada en torno a los 300 Hz. Las antenas para transmitir esta frecuencia deberían tener un tamaño enormemente grande. Esto hace que, para transmitir voz por radio, la señal deba enviarse modulando una señal de frecuencia superior (portadora) para la que la antena correspondiente requiera un tamaño menor.

a) ¿Cuál debe ser la longitud de una antena, equivalente a la mitad de la longitud de onda, para enviar una señal de 300 Hz?

b) Una posible alternativa es emplear algún esquema de modulación, como los descritos en el Capítulo 5, de tal manera que la señal a transmitir tenga un ancho de banda estrecho, centrado en torno a la frecuencia portadora. Supóngase que quisiéramos una antena de 1 metro de longitud. ¿Qué frecuencia de portadora debería utilizarse?

4.8. Hay leyendas sobre gente que es capaz de recibir la señal de radio a través de los empastes de los dientes. Supóngase que tiene un empaste de 2,5 mm (0,0025 m) de largo que actuara a modo de antena, siendo igual su longitud a la mitad de la longitud de onda. ¿Qué frecuencia recibiría?

4.9. Suponga una comunicación entre dos satélites que cumple la ley del espacio libre. Suponga que la señal es muy débil. Se disponen de dos alternativas de diseño. Una consiste en utilizar una frecuencia igual al doble de la frecuencia actual y la otra consiste en duplicar el área efectiva de las dos antenas. Manteniendo todos los demás parámetros inalterados, ¿se conseguirá la misma potencia recibida? o, en caso contrario, ¿cuál de las dos alternativas proporcionaría una potencia recibida superior? ¿Cuál sería el incremento de potencia recibida en el mejor de los casos?

4.10. En la transmisión de radio en el espacio libre, la potencia de la señal se reduce proporcionalmente al cuadrado de la distancia recorrida desde la fuente, mientras que en una transmisión en un cable, la atenuación es una cantidad fija en dB por kilómetro. En la siguiente tabla se muestra, en dB, la reducción relativa a una referencia dada para la transmisión en el espacio libre y en un cable uniforme. Rellene las celdas que faltan para completar la tabla.

Longitud (km)	Radio (dB)	Cable (dB)
1	−6	−3
2		
4		
8		
16		

4.11. En la Sección 4.2 se ha establecido que si una fuente de energía electromagnética se sitúa en el foco de un paraboloide, y que si el paraboloide tiene una superficie reflectante, entonces, la onda se reflejará en líneas paralelas al eje del paraboloide. Para demostrar esto considérese, por ejemplo, la parábola mostrada en la Figura 4.12. Sea $P(x_1, y_1)$ un punto de la parábola y sea PF la línea que une P con el foco. Construya la línea L que pasa por P paralela al eje x y la recta M tangente a la parábola en P. El ángulo entre L y M es β y el ángulo entre PF y M es α. El ángulo α es el ángulo con el que el rayo que pasa por F incide en la parábola en P. Debido a que el ángulo de incidencia es igual al ángulo de reflexión, el rayo reflejado por P debe ser igual al ángulo α. Por tanto, si se demuestra que $\alpha = \beta$, se habrá demostrado que los rayos que se emitan desde F y sean reflejados por la parábola serán paralelos al eje x.

a) Demuestre primero que $\tan \beta = (p/y_1)$. *Sugerencia:* recuérdese de trigonometría que la pendiente de una recta es igual a la tangente del ángulo que forma esa recta con el eje x positivo. Igualmente, recuérdese que la pendiente de una recta tangente a una curva en un punto dado es igual a la derivada de la curva en ese punto.

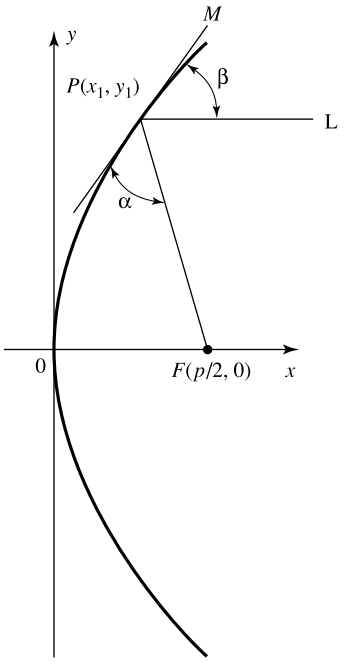


Figura 4.12. Parábola de reflexión.

b) Ahora demuéstrese que $\tan\alpha = (p/y_1)$, lo que demostraría que $\alpha = \beta$. *Sugerencia:* recuérdese de trigonometría que la fórmula de la tangente de la diferencia entre dos ángulos α_1 y α_2, es $\tan(\alpha_2 - \alpha_1) = (\tan\alpha_2 - \tan\alpha_1)/(1 + \tan\alpha_2 \times \tan\alpha_1)$.

4.12. A menudo es más conveniente expresar las distancias en km en lugar de en m y las frecuencias en MHz en lugar de Hz. Rescriba la Ecuación (4.1) usando estas unidades.

4.13. Suponga que un transmisor emite 50 W de potencia.

a) Exprese la potencia transmitida en dBm y dBW.

b) Si la potencia del transmisor se aplica a una antena con ganancia unidad, usando una frecuencia de portadora de 900 MHz, ¿cuál es la potencia recibida, en dBm, en el espacio libre a una distancia de 100 m?

c) Repita el Apartado (b) para una distancia de 10 km.

d) Repita (c) pero suponiendo una ganancia para la antena de recepción de 2.

4.14. Un transmisor de microondas tiene una salida de 0,1 W a 2 GHz. Suponga que este transmisor se utiliza en un sistema de comunicación de microondas en el que las antenas transmisora y receptora son parábolas, cada una con un diámetro igual a 1,2 m.

a) ¿Cuál es la ganancia de cada antena en decibelios?

b) Teniendo en cuenta la ganancia de la antena para la señal transmitida, ¿cuál es la potencia efectiva radiada?

c) Si la antena receptora se sitúa a 24 km de la antena transmisora en el espacio libre, determine la potencia de la señal a la salida de la antena receptora en dBm.

4.15. En la Sección 4.3 se afirma que si no hay obstáculos intermedios, la trayectoria visual óptica se puede expresar como $d = 3{,}75\sqrt{h}$, donde d es la distancia entre la antena y el horizonte, en kilómetros, y h es la altura de la antena, en metros. Teniendo en cuenta que el radio de la Tierra es 6.370 km, obtenga la expresión anterior. *Sugerencia:* supóngase que la antena es perpendicular a la superficie terrestre y nótese que la recta que une el punto más alto de la antena y el horizonte es la tangente a la superficie terrestre en el horizonte. Para visualizar más claramente el problema, dibuje un gráfico con la antena, la trayectoria visual y el radio de la Tierra.

4.16. Calcule la altura de una antena de una emisora de TV que sea capaz de alcanzar clientes alejados a 80 km.

4.17. Suponga que un rayo de luz visible pasa desde la atmósfera hasta el agua formando un ángulo con el horizonte de 30^{o}. ¿Cuál es el ángulo del rayo en el agua? *Nota:* en condiciones atmosféricas normales en la superficie terrestre, un valor razonable del índice de refracción es 1,0003. El valor típico del índice de refracción en el agua es 4/3.

CAPÍTULO 5

Técnicas para la codificación de señales

5.1. Datos digitales, señales digitales
No retorno a cero
Binario multinivel
Bifase
Velocidad de modulación
Técnicas de aleatorización

5.2. Datos digitales, señales analógicas
Modulación por desplazamiento de amplitud
Modulación por desplazamiento de frecuencia
Modulación por desplazamiento de fase
Prestaciones
Modulación de amplitud en cuadratura

5.3. Datos analógicos, señales digitales
Modulación por impulsos codificados
Modulación delta
Prestaciones

5.4. Datos analógicos, señales analógicas
Modulación de amplitud
Modulación angular

5.5. Lecturas recomendadas

5.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- Tanto la información analógica como la digital pueden ser codificadas mediante señales analógicas o digitales. La elección de un tipo particular de codificación dependerá de los requisitos exigidos, del medio de transmisión, así como de los recursos disponibles para la comunicación.
- **Datos digitales, señales digitales:** la forma más sencilla de codificar digitalmente datos digitales es asignar un nivel de tensión al uno binario y otro nivel distinto para el cero. Para mejorar las prestaciones hay que utilizar códigos distintos al anterior, alterando el espectro de la señal y proporcionando capacidad de sincronización.
- **Datos digitales, señales analógicas:** los módem convierten los datos digitales en señales analógicas de tal manera que se puedan transmitir a través de líneas analógicas. Las técnicas básicas son la modulación por desplazamiento de amplitud (ASK), modulación por desplazamiento de frecuencia (FSK) y modulación por desplazamiento de fase (PSK). En todas ellas, para representar los datos digitales, se modifican uno o más parámetros característicos de la señal portadora.
- **Datos analógicos, señales digitales:** los datos analógicos, como por ejemplo la voz y el vídeo, frecuentemente, se digitalizan para ser transmitidos en sistemas digitales. La técnica más sencilla es la modulación por impulsos codificados (PCM) la cual implica un muestreo periódico de los datos analógicos y una cuantización de las muestras.
- **Datos analógicos, señales analógicas:** los datos analógicos se modulan mediante una portadora para generar una señal analógica en una banda de frecuencias diferente, la cual se puede utilizar en un sistema de transmisión analógico. Las técnicas básicas son la modulación de amplitud (AM), la modulación de frecuencia (FM) y la modulación de fase (PM).

En el Capítulo 3 se hizo una diferenciación entre los datos analógicos o digitales y entre lo que son señales analógicas o digitales. En la Figura 3.11 se sugería que ambos tipos de datos se pueden codificar usando cualquiera de los dos tipos de señal.

La Figura 5.1 es otro gráfico en el que se identifican todos los procesos involucrados. En la **señalización digital**, una fuente de datos $g(t)$, que puede ser tanto analógica como digital, se codi-

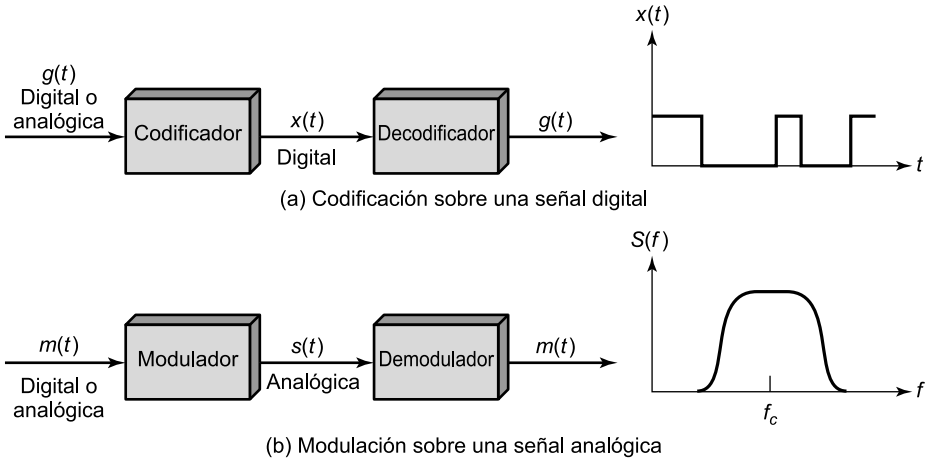


Figura 5.1. Técnicas de codificación y modulación.

fica en una señal digital $x(t)$. La forma de onda en particular que adopte $x(t)$ dependerá de la técnica de codificación elegida, la cual se elegirá intentando optimizar el uso del medio de transmisión. Por ejemplo, la codificación se puede elegir intentando minimizar el ancho de banda o se puede elegir para minimizar la tasa de errores.

La **transmisión analógica** se basa en una señal continua de frecuencia constante denominada **señal portadora**. La frecuencia de la portadora se elige de tal forma que sea compatible con las características del medio que se vaya a utilizar. Los datos se pueden transmitir modulando la señal portadora. La **modulación** es el proceso de codificar los datos generados por la fuente en la señal portadora de frecuencia f_c. Todas las técnicas de modulación se basan en la modificación de uno o más de los tres parámetros fundamentales que caracterizan a la portadora en el dominio de la frecuencia: la amplitud, la frecuencia y la fase.

La señal de entrada $m(t)$ (que puede ser tanto analógica como digital) se denomina señal moduladora o, también, **señal en banda base**. A la señal resultante de la modulación de la portadora se le denomina señal modulada $s(t)$. Como se indica en la Figura 5.1b, $s(t)$ es una señal limitada en banda (pasobanda). La localización del ancho de banda dependerá de f_c ya que, por lo general, estará centrado en torno a ésta. De nuevo, el procedimiento de codificación se elegirá intentando optimizar algunas de las características de la transmisión.

Cada una de las cuatro posibles combinaciones mostradas en la Figura 5.1 se utilizan ampliamente; si bien, las razones por las que se elige una u otra, en una transmisión determinada, dependerán de varios factores, como los que se indican a continuación:

- **Datos digitales, señales digitales:** en términos generales, el equipamiento para la codificación digital usando señales digitales es menos complejo y menos costoso que el equipamiento utilizado para transmitir datos digitales usando señales analógicas mediante modulación.
- **Datos analógicos, señales digitales:** la conversión de los datos analógicos a digitales permite la utilización de técnicas de transmisión y de equipos de conmutación modernos. Las ventajas de la aproximación digital se describieron en la Sección 3.2.
- **Datos digitales, señales analógicas:** algunos medios de transmisión, como por ejemplo la fibra óptica o los medios no guiados, sólo permiten la propagación de señales analógicas.
- **Datos analógicos, señales analógicas:** los datos analógicos de naturaleza eléctrica se pueden transmitir fácilmente y con bajo coste en banda base. Esto es lo que se hace, por ejemplo, en la transmisión de voz en las líneas de calidad telefónica. La modulación se usa frecuentemente para desplazar el ancho de banda de la señal en banda base hacia otra zona del espectro. De esta manera, se permite que varias señales, cada una en una posición diferente del espectro, compartan el mismo medio de transmisión. Este procedimiento se denomina multiplexación por división en frecuencias.

A continuación, se examinarán las técnicas involucradas en las cuatro combinaciones anteriores.

5.1. DATOS DIGITALES, SEÑALES DIGITALES

Una señal digital es una secuencia de pulsos de tensión discretos y discontinuos. Cada pulso es un elemento de señal. Los datos binarios se transmiten codificando cada bit en los elementos de señal. En el caso más sencillo, habrá una correspondencia uno a uno entre los bits y dichos elementos. En la Figura 3.16 se muestra un ejemplo en el que un 1 binario se representa mediante un nivel bajo de tensión y un 0 binario se representa por un nivel de tensión mayor. En esta sección se mostrará

que, además de la mostrada en la figura mencionada, hay una gran cantidad de alternativas para la codificación.

En primer lugar, se va a introducir un poco de terminología. Si todos los elementos de señal tienen el mismo signo algebraico (es decir, si son todos positivos o todos negativos) la señal es **unipolar**. En una señal **polar**, por el contrario, un estado lógico se representará mediante un nivel positivo de tensión y el otro mediante un nivel negativo. La **velocidad de transmisión de una señal**, o simplemente **la velocidad de transmisión**, es la velocidad, expresada en bits por segundo, a la que se transmiten los datos. Se define la duración o longitud de un bit como el tiempo empleado en el transmisor para emitir un bit; para una velocidad de transmisión R, la duración de un bit será $1/R$. La **velocidad de modulación**, por el contrario, es la velocidad a la que cambia el nivel de la señal, que como se explicará más adelante, dependerá del esquema de codificación elegido. La velocidad de modulación se expresa en baudios, que equivale a un elemento de señal por segundo. Para concluir, por razones históricas, se usan los términos «marca» y «espacio» aludiendo a los dígitos binarios 1 y 0 respectivamente. En la Tabla 5.1 se resume la terminología aquí introducida, que se aclarará posteriormente en esta sección mediante un ejemplo.

Tabla 5.1. Terminología básica en transmisión de datos.

Término	Unidades	Definición
Datos	Bits	Un valor binario cero o uno
Velocidad de transmisión	Bits por segundo (bps)	Velocidad a la que se transmiten los datos
Elemento de señal	Digital: pulso de tensión de amplitud constante. Analógico: pulso de frecuencia, fase y amplitud constantes	Parte de la señal correspondiente al código de señalización más corto
Velocidad de modulación o de señalización	Elementos de señal por segundo (baudios).	Velocidad a la que se transmiten los elementos de señal

Las tareas involucradas al interpretar las señales digitales en el receptor se pueden resumir de nuevo considerando la Figura 3.16. En primer lugar, el receptor debe conocer o determinar la duración de cada bit. Es decir, el receptor, con mayor o menor precisión, debe conocer cuándo comienza y cuándo acaba cada bit. En segundo lugar, el receptor debe determinar si el nivel de cada bit es alto (0) o bajo (1). En la Figura 3.16, estas tareas se realizan muestreando a la mitad del intervalo temporal que ocupa cada bit y comparando posteriormente el valor obtenido con un umbral. Debido a la existencia de ruido y otros defectos en la transmisión puede que haya errores, como se muestra en la mencionada figura.

¿Qué factores determinan el éxito o el fracaso del receptor al interpretar la señal de entrada? Ya se vio en el Capítulo 3 que hay tres factores importantes: la relación señal ruido (o mejor, el cociente E_b/N_0), la velocidad de transmisión y el ancho de banda. Si se suponen los otros factores constantes, se puede afirmar que:

- Un incremento en la velocidad de transmisión aumentará la tasa de errores por bit (BER, *Bit Error Rate*)[1].

[1] BER es la medida más habitual para determinar la cantidad de errores en cualquier línea de transmisión de datos; se define como la probabilidad de que un bit se reciba erróneamente. También se denomina *fracción de errores por bit*. Este

- Un aumento en la relación SNR reduce la tasa de errores por bit.
- Un incremento del ancho de banda permite un aumento en la velocidad de transmisión.

Hay otro factor que se puede utilizar para mejorar las prestaciones del sistema, el cual no es otro sino el propio esquema de codificación. El esquema de codificación es simplemente la correspondencia que se establece entre los bits de los datos con los elementos de señal. Se han intentado una gran diversidad de aproximaciones. En lo que sigue, se describen algunas de las más utilizadas; éstas se definen en la Tabla 5.2 y se muestran en la Figura 5.2.

Tabla 5.2. Definición de los formatos para la codificación de señales digitales.

No retorno a nivel cero (NRZ-L)
0 = nivel alto
1 = nivel bajo

No retorno a cero invertido (NRZI)
0 = no hay transición al comienzo del intervalo (un bit cada vez)
1 = transición al comienzo del intervalo

Bipolar-AMI
0 = no hay señal
1 = nivel positivo o negativo, alternante

Pseudoternaria
0 = nivel positivo a negativo, alternante
1 = no hay señal

Manchester
0 = transición de alto a bajo en mitad del intervalo
1 = transición de bajo a alto en mitad del intervalo

Manchester diferencial
Siempre hay una transición en mitad del intervalo
0 = transición al principio del intervalo
1 = no hay transición al principio del intervalo

B8ZS
Igual que el bipolar-AMI, excepto que cualquier cadena de ocho ceros se reemplaza por una cadena que tiene dos violaciones de código.

HDB3
Igual que el bipolar-AMI, excepto que cualquier cadena de cuatro ceros se reemplaza por una cadena que contiene una violación de código.

Antes de describir las técnicas de codificación propiamente dichas, a continuación se consideran los siguientes procedimientos a tener en cuenta para su evaluación y comparación.

- **Espectro de la señal:** hay varios aspectos del espectro de la señal que son importantes. La ausencia de componentes a altas frecuencias significa que se necesita menos ancho de banda para su transmisión. Es más, la ausencia de componente en continua (dc) es también una característica deseable. Si la señal tiene continua, para su transmisión se requiere la existencia de una conexión física directa; si la señal no contiene componente continua, es posible su transmisión mediante transformadores acoplados. De esta manera, se proporciona un aislamiento eléctrico excelente y se reducen las interferencias. Por último, la importancia de los

último término es más esclarecedor, ya que el término *tasa* se refiere normalmente a una cantidad que varía con el tiempo. Desgraciadamente, la mayoría de los libros y documentos de normalización consideran a la *R* de BER como *Rate* (tasa) y no como *Ratio* (fracción).

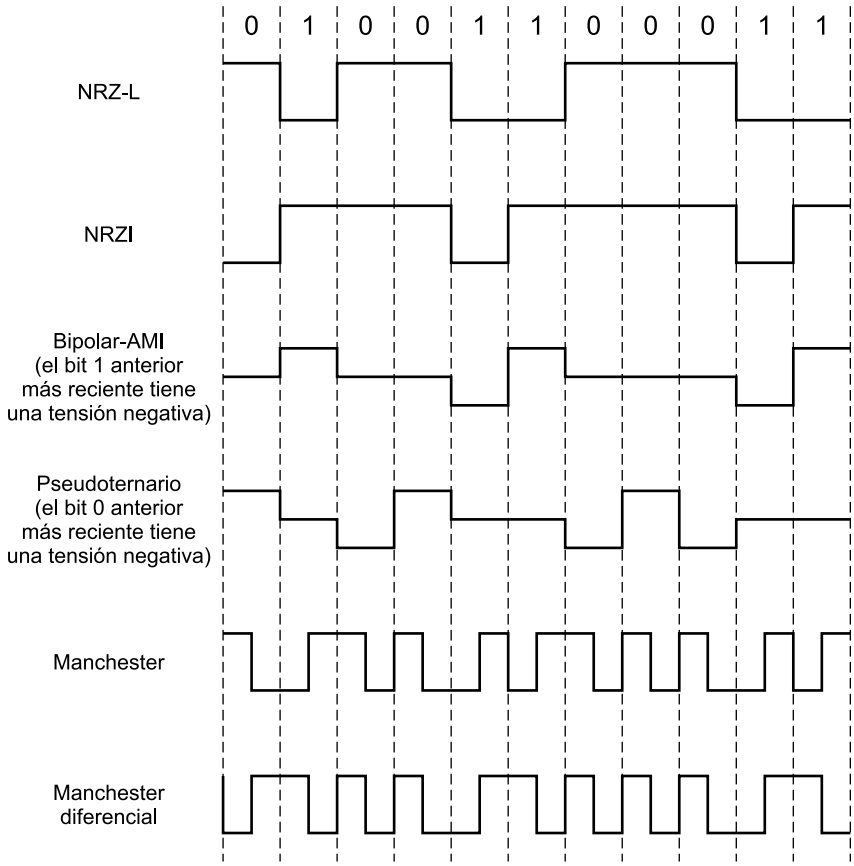


Figura 5.2. Formatos de codificación utilizando señales digitales.

efectos relacionados con la distorsión de la señal y las interferencias depende de las propiedades espectrales de la señal transmitida. En la práctica, es frecuente que la función de transferencia del canal se deteriore en las proximidades de los límites de la banda. Por tanto, un buen diseño debería concentrar la potencia transmitida en la parte central del ancho de banda de la señal transmitida. En tal caso, se tendrá una distorsión menor en la señal recibida. Para conseguir este objetivo, los códigos se pueden diseñar de forma que se modifique adecuadamente el espectro de la señal transmitida.

- **Sincronización:** ya se ha mencionado la necesidad de determinar el principio y fin de cada bit. Esto no es una tarea fácil. Una solución, bastante costosa, es transmitir una señal de reloj por separado para sincronizar el receptor con el transmisor. Una alternativa es proporcionar la sincronización mediante la propia señal transmitida, lo que puede conseguirse si se adopta un esquema de codificación adecuado.
- **Detección de errores:** en el Capítulo 6 se discutirán algunas de las técnicas que se usan para la detección de errores y, además, se mostrará que estas técnicas son responsabilidad de una capa situada encima del nivel de señalización, denominada control del enlace de datos. No obstante, es útil incorporar alguna capacidad de detección de errores en el propio esquema de codificación, situado en la capa física, permitiéndose así que los errores se detecten más rápidamente.

- **Inmunidad al ruido e interferencias:** algunos códigos exhiben un comportamiento superior que otros en presencia de ruido. Las prestaciones se expresan habitualmente mediante la BER.
- **Coste y complejidad:** aunque el coste económico de la lógica digital continúa bajando, no se debe ignorar este factor. En particular, cuanto mayor es la velocidad de modulación para una velocidad de transmisión dada, mayor es el coste. En lo que sigue se describirán algunos códigos que implican una velocidad de modulación superior a la velocidad de transmisión de datos real.

Volvamos ya a la presentación y discusión de los diversos esquemas de codificación.

NO RETORNO A CERO

La forma más frecuente y fácil de transmitir señales digitales es mediante la utilización de un nivel diferente de tensión para cada uno de los dos dígitos binarios. Los códigos que siguen esta estrategia comparten la propiedad de que el nivel de tensión se mantiene constante durante la duración del bit; es decir, no hay transiciones (no hay retorno al nivel cero de tensión). Por ejemplo, la ausencia de tensión se puede usar para representar un 0 binario, mientras que un nivel constante y positivo de tensión puede representar al 1. Este código se denomina no retorno a cero (NRZ, *Nonreturn to Zero*). Sin embargo, es más habitual usar un nivel negativo para representar un valor binario y una tensión positiva para representar al otro. Este último código, mostrado[2] en la Figura 5.2, se denomina código **no retorno a nivel cero** (NRZ-L, *Nonreturn to Zero-Level*). NRZ-L se usa generalmente para generar o interpretar los datos binarios en terminales y otros dispositivos. Si se utiliza un código diferente, éste se generará usualmente a partir de la señal NRZ-L —en los términos que se muestran en la Figura 5.1, la señal NRZ-L es $g(t)$ y la señal codificada es $x(t)$—.

Una variante del NRZ se denomina **NRZI** (*Noreturn to Zero*, *invert on ones*). Al igual que NRZ-L, NRZI mantiene constante el nivel de tensión durante la duración de un bit. Los datos se codifican mediante la presencia o ausencia de una transición de la señal al principio del intervalo de duración del bit. Un 1 se codifica mediante la transición (bajo a alto o alto a bajo) al principio del intervalo de señalización, mientras que un cero se representa por la ausencia de transición.

NRZI es un ejemplo de **codificación diferencial**. En la codificación diferencial, en lugar de determinar el valor absoluto, la señal se decodifica en función de los cambios entre los elementos de señal adyacentes. En términos generales, la codificación de cada bit se hace de la siguiente manera: si se trata del valor binario 0, se codifica con la misma señal que el bit anterior; si se trata de un valor binario 1, entonces se codifica con una señal diferente que la utilizada para el bit precedente. Una ventaja de este esquema es que en presencia de ruido puede ser más seguro detectar una transición en lugar de comparar un valor con un umbral. Otra ventaja es que en un sistema de transmisión complejo, no es difícil perder la polaridad de la señal. Por ejemplo, en una línea de par trenzado, si los cables se invierten accidentalmente, se invertirán todos los 1 y 0 en NRZ-L. Esto no pasa en un esquema diferencial.

Los códigos NRZ son los más fáciles de implementar y, además, se caracterizan por hacer un uso eficaz del ancho de banda. Esta última propiedad se pone de manifiesto en la Figura 5.3, en la que se compara la densidad espectral de varios esquemas de codificación. En dicha figura, la fre-

[2] En esta figura, una tensión negativa representa un 1 binario y una positiva representa un 0. Esta definición es posiblemente contraria a la definición utilizada en otros textos. La definición aquí presentada es coherente con la usada en NRZ-L en las interfaces de comunicaciones de datos y en las normalizaciones que controlan dichas interfaces.

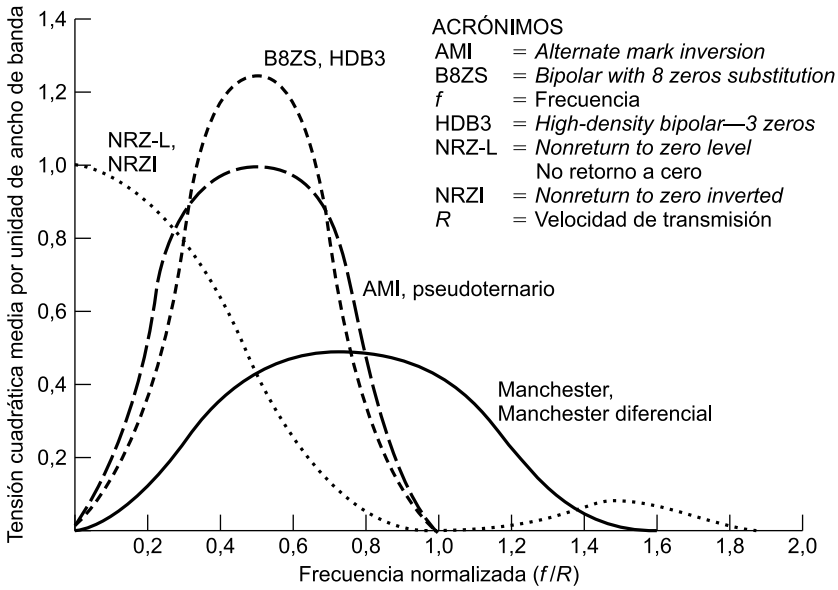


Figura 5.3. Densidad espectral de varios esquemas de codificación.

cuencia está normalizada a la velocidad de transmisión de los datos. Como se puede ver, en los códigos NRZ y NRZI la mayor parte de la energía está comprendida entre la componente continua y la mitad de la velocidad de transmisión. Por ejemplo, si se usa un código NRZ para generar una señal a una velocidad de transmisión de 9.600 bps, la mayor parte de la energía estará concentrada entre la componente continua (dc) y 4.800 Hz.

La principal limitación de las señales NRZ es la presencia de una componente dc continua y la ausencia de capacidad de sincronización. Para ilustrar esta última desventaja, téngase en cuenta que una cadena larga de unos o de ceros en un esquema NRZ-L, o una cadena de ceros en el NRZI, se codificará como un nivel de tensión constante durante un intervalo de tiempo largo. En estas circunstancias, cualquier fluctuación entre los relojes del transmisor y el receptor dará lugar a una pérdida de sincronización entre ambos.

Debido a su sencillez y a las características de su respuesta en frecuencias relativamente bajas, los códigos NRZ se usan normalmente en las grabaciones magnéticas. No obstante, sus limitaciones hacen que estos códigos no sean atractivos para aplicaciones de transmisión de señales.

BINARIO MULTINIVEL

Las técnicas de codificación denominadas binario multinivel subsanan algunas de las deficiencias mencionadas para los códigos NRZ. Estos códigos usan más de dos niveles de señal. En la Figura 5.2 se muestran dos ejemplos, el bipolar-AMI (*Alternate Mark Inversion*) y el pseudoternario[3].

[3] Estos términos no se usan con consistencia en la bibliografía. En algunos textos, estos dos términos se usan para esquemas de codificación diferentes a los aquí definidos e, igualmente, para los códigos mostrados en la Figura 5.2 se usa una gran diversidad de términos. La nomenclatura que se ha adoptado corresponde con la utilizada en varios estándares de la UIT-T.

En el caso del esquema **bipolar-AMI**, un 0 binario se representa por ausencia de señal y el 1 binario se representa como un pulso positivo o negativo. Los pulsos correspondientes a los 1 deben tener una polaridad alternante. Este tipo de esquema tiene las siguientes ventajas. En primer lugar, no habrá problemas de sincronización en el caso de que haya una cadena larga de unos. Cada 1 fuerza una transición, por lo que el receptor se puede sincronizar en dicha transición. Una cadena larga de ceros sigue siendo un problema. En segundo lugar, ya que los elementos de señal correspondientes a 1 alternan el nivel de tensión, no hay componente continua. Además, el ancho de banda de la señal resultante es considerablemente menor que el correspondiente a NRZ (*véase* Figura 5.3). Por último, la alternancia entre los pulsos proporciona una forma sencilla de detectar errores. Cualquier error aislado, tanto si elimina como si introduce un pulso, implica un incumplimiento de dicha propiedad.

Los comentarios del párrafo anterior son también trasladables a los códigos **pseudoternarios**. En este caso, el bit 1 se representa por la ausencia de señal y el 0 mediante pulsos de polaridad alternante. No hay ninguna ventaja particular de esta codificación respecto de la anterior, siendo la base de muchas aplicaciones.

No obstante, el grado de sincronización proporcionado por estos códigos todavía presenta algunos problemas (una cadena larga de ceros en el caso del AMI, o de unos en el pseudoternario). Para solventar dichos problemas se han propuesto otros códigos. Una posibilidad es insertar bits que fuercen transiciones. Este procedimiento se adopta en RDSI para la transmisión a velocidades relativamente bajas. Desde luego, este esquema es costoso para velocidades de transmisión superiores, ya que significaría un aumento en la, ya de por sí, alta velocidad de transmisión. Para resolver este problema a altas velocidades de transmisión se utiliza una técnica que implica desordenar o revolver los datos (técnicas de aleatorización, en inglés *scrambling*). Posteriormente, en esta sección se proporcionarán dos ejemplos de esta técnica.

Así pues, con las modificaciones pertinentes, el esquema binario multinivel soslaya los problemas de los códigos NRZ. Por supuesto, al igual que en cualquier otra decisión de ingeniería, siempre existe un compromiso. Con la codificación binaria multinivel, la señal puede tomar tres posibles valores en cada elemento de señal, lo que representaría $\log_2 3 = 1{,}58$ bits de información, aunque en realidad transporta sólo un bit de información. Por tanto, el código binario multinivel no es tan eficaz como los NRZ. Otra forma de enunciar este hecho es que el receptor de señales codificadas con binario multinivel se ve obligado a distinguir entre tres niveles ($+A$, $-A$, 0), en lugar de los dos niveles de los otros esquemas presentados anteriormente. Por tanto, para obtener la misma probabilidad de error, la señal de un código binario multinivel necesita aproximadamente 3 dB más de potencia que las señales bivaluadas. Este hecho se muestra en la Figura 5.4. Dicho de otra forma, dada una relación señal ruido, la tasa de errores por bit para los códigos NRZ es significativamente menor que la correspondiente en un código binario multinivel.

BIFASE

Bajo el término *bifase* se engloba a un conjunto de técnicas de codificación alternativas diseñadas para superar las dificultades encontradas en los códigos NRZ. Dos de estas técnicas, denominadas Manchester y Manchester diferencial, se usan frecuentemente en los sistemas de comunicación.

En el código **Manchester**, siempre hay una transición en mitad del intervalo de duración del bit. Esta transición en la mitad del bit sirve como procedimiento de sincronización, a la vez que sirve para transmitir los datos: una transición de bajo a alto representa un 1 y una transición de alto

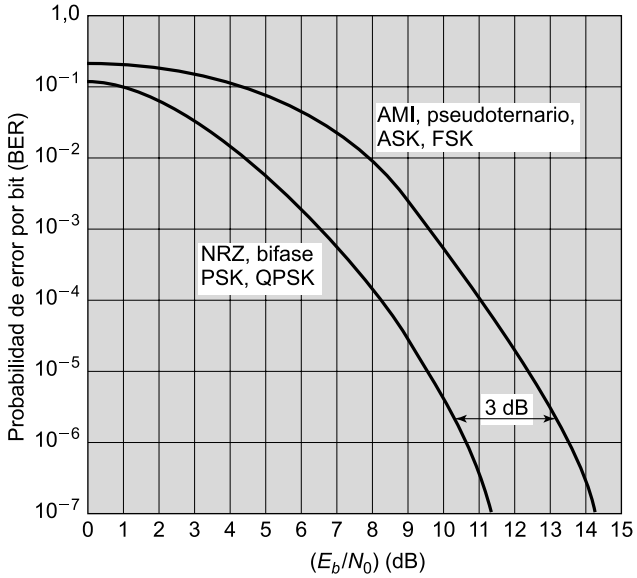


Figura 5.4. Tasas de error por bit teóricas para varios esquemas de codificación digital.

a bajo representa un 0[4]. En **Manchester diferencial**, la transición a mitad del intervalo se utiliza tan sólo para proporcionar sincronización. La codificación de un 0 se representa por la presencia de una transición al principio del intervalo del bit, y un 1 se representa mediante la ausencia de una transición al principio del intervalo. El código Manchester diferencial tiene como ventajas adicionales las derivadas de la utilización de una aproximación diferencial.

Todas las técnicas bifase fuerzan al menos una transición por cada bit pudiendo tener hasta dos en ese mismo periodo. Por tanto, la velocidad de modulación máxima es el doble que en los códigos NRZ; esto significa que el ancho de banda necesario es por tanto mayor. No obstante, los esquemas bifase tienen las siguientes ventajas:

- **Sincronización:** debido a que la transición que ocurre durante el intervalo de duración correspondiente a un bit siempre está presente, el receptor puede sincronizarse usando dicha transición. Por esta razón a los códigos bifase también se les denomina autosincronizados.
- **No tienen componente en continua:** los códigos bifase no tienen componente en continua, lo que implica todas las ventajas mencionadas anteriormente.
- **Detección de errores:** se pueden detectar errores si se descubre una ausencia de la transición esperada en mitad del intervalo. Para que el ruido produjera un error no detectado tendría que invertir la señal antes y después de la transición.

Como se puede ver en la Figura 5.3, el ancho de banda en los códigos bifase es razonablemente estrecho, además no contiene componente continua. Aun así, es más ancho que el ancho de banda de los códigos binarios multinivel.

[4] La definición del código Manchester presentada aquí es opuesta a la que se usa en muchos libros de texto prestigiosos (por ejemplo: [TANE03], [KURO01], [LEON00], [WALR00] y [PETE00]) en los que un 0 binario corresponde a una transición bajo a alto, y un 1 binario corresponde a una transición alto a bajo. Aquí, la definición adoptada es coherente con la definición adoptada en varios estándares para LAN, como por ejemplo la norma IEEE 802.3.

Los códigos bifase se usan con frecuencia en los esquemas de transmisión de datos. Uno de los más conocidos es el código Manchester, elegido como parte de la especificación de la norma IEEE 802.3 (Ethernet) para la transmisión en redes LAN de cable coaxial en banda base o par trenzado con bus CSMA/CD. El Manchester diferencial se ha elegido en la norma IEEE 802.5 para redes LAN en anillo con paso de testigo, en las que se usan pares trenzados apantallados.

VELOCIDAD DE MODULACIÓN

Cuando se usan técnicas de codificación de señales, se debe hacer una diferenciación entre la velocidad de transmisión de los datos (expresada en bits por segundo) y la velocidad de modulación (expresada en baudios). La velocidad de transmisión, también denominada tasa de bits, es $1/T_B$, donde T_B = duración de un bit. La velocidad de modulación es aquella a la que se generan los elementos de señal. Considérese, por ejemplo, la codificación Manchester. El elemento de señal mínimo tiene una duración igual a la mitad de la duración del intervalo correspondiente a un bit. Si se tratara de una cadena de bits todos iguales a 0, o a 1, se generaría una serie de pulsos como los mencionados. Por tanto, la velocidad máxima de modulación en el código Manchester es $2/T_B$. Este caso se muestra en la Figura 5.5, correspondiente a la transmisión de una cadena de unos a una velocidad de transmisión igual a 1 Mbps usando NRZI y Manchester. En general,

$$D = \frac{R}{L} = \frac{R}{\log_2 M} \tag{5.1}$$

donde

D = velocidad de modulación en baudios.

R = velocidad de transmisión en bps.

M = número de elementos de señalización diferentes = 2^L.

L = número de bits por elemento de señal.

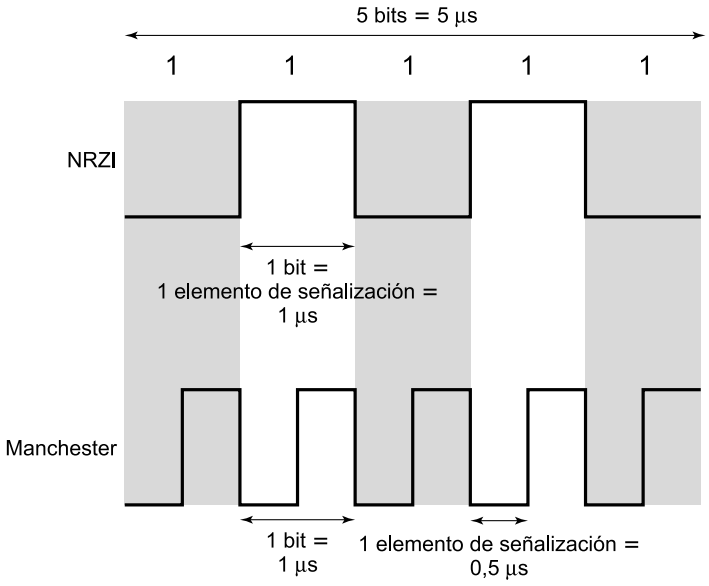


Figura 5.5. Una cadena de unos a 1 Mbps.

Una forma de caracterizar la velocidad de modulación es determinando el número medio de transiciones que se dan en el intervalo de tiempo correspondiente a la duración de un bit. En general, esto dependerá de la secuencia en particular de bits que se transmitan. En la Tabla 5.3 se comparan las velocidades de modulación para diversas técnicas. En dicha tabla se indican las velocidades de transición de la señal normalizadas para el caso de una cadena de unos y ceros alternantes, así como para las cadenas de datos correspondientes a la velocidad de modulación máxima y mínima.

Tabla 5.3. Velocidades normalizadas de transición de la señal, para varios esquemas de codificación de señales digitales.

	Mínimo	101010...	Máximo
NRZ-L	0 (todo 0 o 1)	1,0	1,0
NRZI	0 (todo 0)	0,5	1,0 (todo 1)
Bipolar-AMI	0 (todo 0)	1,0	1,0
Pseudoternario	0 (todo 1)	1,0	1,0
Manchester	1,0 (1010...)	1,0	2,0 (todo 0 o 1)
Manchester diferencial	1,0 (todo 1)	1,5	2,0 (todo 0)

TÉCNICAS DE ALEATORIZACIÓN

El éxito obtenido por los esquemas bifase en el entorno de las redes LAN a velocidades relativamente altas (hasta 10 Mbps), no es trasladable a las redes de larga distancia. La razón principal estriba en el hecho de que la bifase requiere una alta velocidad de modulación comparada con la velocidad de transmisión obtenida para los datos. Este tipo de desventaja es más relevante, y por tanto más costosa, en redes de larga distancia.

Un enfoque alternativo, denominado aleatorización, consiste en utilizar alguna técnica que desordene la información. La idea subyacente en este tipo de técnicas es sencilla: reemplazar las secuencias de bits que den lugar a niveles de tensión constante por otras secuencias que proporcionen suficiente número de transiciones, de tal forma que el reloj del receptor pueda mantenerse sincronizado. En el receptor se debe identificar la secuencia reemplazada y sustituirla por la secuencia original. La secuencia reemplazada tendrá la misma longitud que la original. Por tanto, este procedimiento no implica penalización en la velocidad de transmisión de los datos. Los objetivos en el diseño de estas técnicas, se pueden resumir en:

- Evitar la componente en continua.
- Evitar las secuencias largas que correspondan a niveles de tensión nula.
- No reducir la velocidad de transmisión de los datos.
- Tener capacidad para detectar errores.

En la Figura 5.6 se muestran dos de las técnicas que se usan frecuentemente en las comunicaciones a larga distancia.

Un esquema de codificación que se usa habitualmente en Norteamérica se denomina bipolar con sustitución de ocho ceros (**B8ZS, *Bipolar with 8-Zeros Substitution***) el cual se basa en un

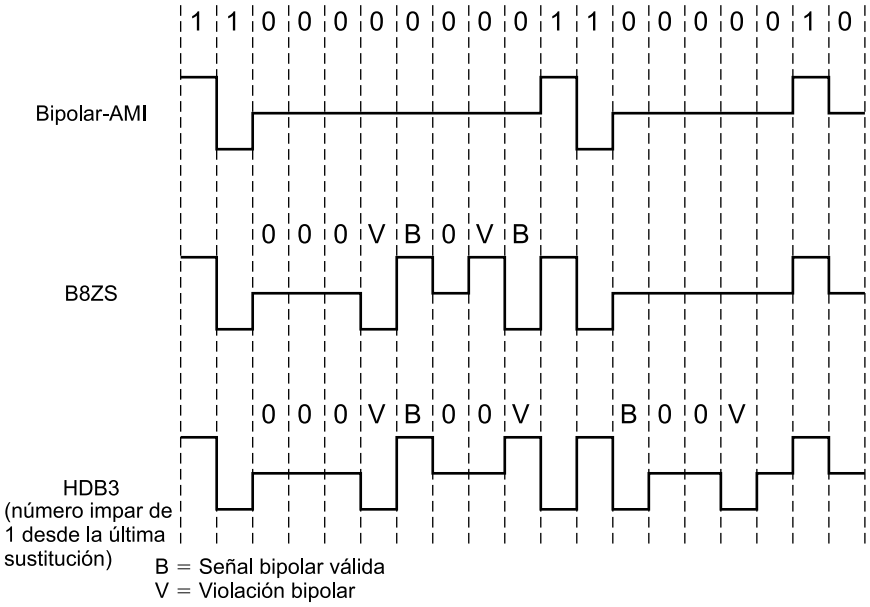

1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0
Bipolar-AMI
0 0 0 V B 0 V B
B8ZS
0 0 0 V B 0 0 V B 0 0 V
HDB3
(número impar de
1 desde la última
sustitución)
B = Señal bipolar válida
V = Violación bipolar

Figura 5.6. Reglas de codificación para B8ZS y HDB3.

AMI bipolar. Previamente se ha mencionado que el inconveniente de los códigos AMI es que una secuencia larga de ceros puede dar lugar a una pérdida de sincronización. Para evitar este problema, la codificación se realiza de acuerdo con las siguientes reglas:

- Si aparece un octeto con todo ceros y el último valor de tensión anterior a dicho octeto fue positivo, dicho octeto se codifica como $000+-0-+$.
- Si aparece un octeto con todo ceros y el último valor de tensión anterior a dicho octeto fue negativo, dicho octeto se codifica como $000-+0+-$.

Con este procedimiento se fuerzan dos violaciones de código (esto es, combinaciones de estados de señalización no permitidos por el código) del código AMI. Estas dos violaciones tienen una probabilidad muy baja de haber sido causadas por el ruido u otros defectos en la transmisión. Por tanto, el receptor identificará ese patrón y lo interpretará convenientemente como un octeto todo ceros.

Un esquema de codificación que se utiliza habitualmente en Europa y Japón es el denominado bipolar de alta densidad de tres ceros (**HDB3, *High Density Bipolar-3 Zeros*), (***véase*** Tabla 5.4). Al igual que el anterior, se basa en la codificación AMI. En este esquema, las cadenas de cuatro ceros se reemplazan por cadenas que contienen uno o dos pulsos. En este caso, el cuarto cero se sustituye por una violación del código. Además, en las violaciones siguientes, se considera una

Tabla 5.4. Reglas de sustitución en HDB3.

	Número de pulsos bipolares (unos) desde la última sustitución	
Polaridad del pulso anterior	**Impar**	**Par**
−	000−	+00+
+	000+	−00−

regla adicional para asegurar que las mismas tengan una polaridad alternante, evitando así la introducción de componente continua. Es decir, si la última violación fue positiva la siguiente deberá ser negativa, y viceversa. En la Tabla 5.4 se indica que esta condición se determina dependiendo de (1) si el número de pulsos desde la última violación es par o impar, y (2) dependiendo de la polaridad del último pulso anterior a la aparición de los cuatro ceros.

En la Figura 5.3 se muestran las propiedades espectrales de los dos códigos mencionados. Como se puede observar, ninguno de los dos contiene componente de continua. La mayor parte de la energía se concentra en una región estrecha en torno a la frecuencia correspondiente a la mitad de la velocidad de transmisión. Por tanto, estos códigos son adecuados para la transmisión a altas velocidades.

5.2. DATOS DIGITALES, SEÑALES ANALÓGICAS

Consideremos ahora el caso de la transmisión de datos digitales usando señales analógicas. La situación más habitual para este tipo de comunicaciones es la transmisión de datos digitales a través de la red de telefonía pública. Esta red se diseñó para recibir, conmutar y transmitir señales analógicas en el rango de frecuencias de voz entre 300 y 3.400 Hz. No es adecuada, por tanto, para la transmisión de señales digitales desde el terminal de abonado (aunque esto está cambiando progresivamente). No obstante, se pueden conectar dispositivos digitales a través de la red mediante el uso de dispositivos módem (modulador-demodulador), los cuales convierten los datos digitales en señales analógicas y viceversa.

En la red telefónica los módem se usan para que las señales estén en el rango de frecuencias de la voz, si bien, las mismas técnicas se pueden usar para módem a frecuencias más altas (por ejemplo, microondas). En esta sección se presentan estas técnicas y se proporciona una breve discusión de las prestaciones de las distintas alternativas posibles.

Como ya se ha comentado previamente, la modulación implica la modificación de uno o varios de los tres parámetros fundamentales que caracterizan a la señal portadora: la amplitud, la frecuencia o la fase. Consecuentemente, hay tres técnicas básicas de codificación o, mejor dicho, de modulación que transforman los datos digitales en señales analógicas, como se muestra en la Figura 5.7: modulación por desplazamiento de amplitud (ASK, *Amplitude Shift Keying*), modulación por desplazamiento de frecuencia (FSK, *Frequency-Shift Keying*) y modulación por desplazamiento de fase (PSK, *Phase-Shift Keying*). En todos los casos, la señal resultante ocupa un ancho de banda centrado en torno a la frecuencia de la portadora.

MODULACIÓN POR DESPLAZAMIENTO DE AMPLITUD

En ASK, los dos valores binarios se representan mediante dos amplitudes diferentes de la portadora. Es usual que una de las amplitudes sea cero; es decir, uno de los dígitos binarios se representa mediante la presencia de la portadora a amplitud constante y el otro mediante la ausencia de portadora (*véase* Figura 5.7a). La señal transmitida por cada intervalo correspondiente a la duración de un bit es, por tanto:

$$\textbf{ASK} \qquad s(t) = \begin{cases} A\cos(2\pi f_c t) & 1 \text{ binario} \\ 0 & 0 \text{ binario} \end{cases} \tag{5.2}$$

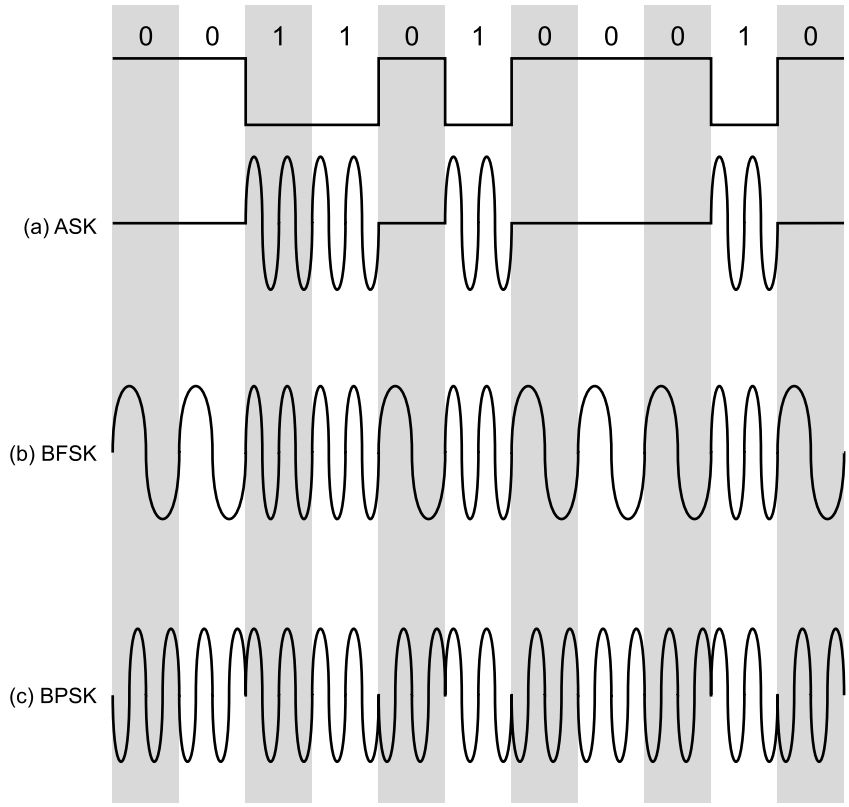


Figura 5.7. Modulación de datos digitales usando señales analógicas.

en la que la portadora es $A\cos(2\pi f_c t)$. ASK es sensible a cambios repentinos de la ganancia. Además, es una técnica de modulación bastante ineficaz. En líneas de calidad telefónica, ASK se usa en el mejor de los casos a 1.200 bps.

La técnica ASK se usa para la transmisión de datos digitales en fibras ópticas. En los transmisores con LED, la Ecuación (5.2) sigue siendo válida. Es decir, un elemento de señal se representa mediante un pulso de luz, mientras que el otro elemento se representa mediante la ausencia de luz. Los transmisores láser tienen normalmente un valor fijo de la corriente de polarización (*current bias*) que hace que el dispositivo emita, para el último caso, una señal de baja intensidad. Este pequeño nivel será uno de los elementos de señalización, mientras que el otro será un haz de luz de mayor amplitud.

MODULACIÓN POR DESPLAZAMIENTO DE FRECUENCIA

El esquema FSK más habitual es el binario, BFSK (*binary FSK*). En este caso, los dos valores binarios se representan mediante dos frecuencias diferentes, próximas a la frecuencia de la portadora (*véase* Figura 5.7b). La señal transmitida en cada intervalo correspondiente a la duración de un bit será

$$\textbf{BFSK} \qquad s(t) = \begin{cases} A\cos(2\pi f_1 t) & 1 \text{ binario} \\ A\cos(2\pi f_2 t) & 0 \text{ binario} \end{cases} \tag{5.3}$$

donde f_1 y f_2 corresponden a desplazamientos de la frecuencia portadora f_c, de igual magnitud, pero en sentidos opuestos.

En la Figura 5.8 se muestra un ejemplo del uso de BFSK en una transmisión *full-duplex* en una línea de calidad telefónica. Dicha figura corresponde con la especificación de la serie de módem Bell System 108. Recuérdese que una línea de calidad telefónica deja pasar frecuencias en el rango aproximado de 300 a 3.400 Hz y que *full-duplex* significa que las señales se transmiten simultáneamente en ambos sentidos. Para transmitir en *full-duplex*, el ancho de banda anterior se divide en dos. En uno de los sentidos (correspondiente a la transmisión o a la recepción) las frecuencias utilizadas para representar al 1 o 0 están centradas en torno a 1.170 Hz, desplazándose 100 Hz a cada lado. El efecto de usar estas dos frecuencias corresponde a la transmisión de una señal cuyo espectro corresponde con la zona sombreada de la izquierda de la Figura 5.8. De igual manera, para el otro sentido (recepción o transmisión) el módem utilizará señales correspondientes a desplazamientos de 100 Hz en torno a la frecuencia central de 2.125 Hz. Estas señales corresponden con el área sombreada de la derecha en la Figura 5.8. Obsérvese que hay un pequeño solapamiento entre las bandas, es decir, hay una pequeña interferencia.

BFSK es menos sensible a errores que ASK. En líneas de calidad telefónica, se utiliza generalmente a velocidades de hasta 1.200 bps. También se usa frecuentemente en transmisión de radio a más altas frecuencias (desde 3 hasta 30 MHz). También se puede usar incluso a frecuencias superiores en redes de área local que utilicen cable coaxial.

Una señal más eficaz en el uso del ancho de banda, pero también más susceptible a errores, es la FSK múltiple (MFSK, *Multiple FSK*), en la que se usan más de dos frecuencias. En este caso, cada elemento de señalización representará más de un bit. La señal MFSK transmitida durante el intervalo correspondiente a un elemento de señalización se define como:

$$\textbf{MFSK} \qquad s_i(t) = A\cos 2\pi f_i t, \qquad 1 \leqslant i \leqslant M \tag{5.4}$$

donde

$f_i = f_c + (2i - 1 - M)f_d$

f_c = la frecuencia de la portadora.

f_d = la diferencia de frecuencias.

M = el número de elementos de señalización diferentes.

L = el número de bits por elemento de señalización.

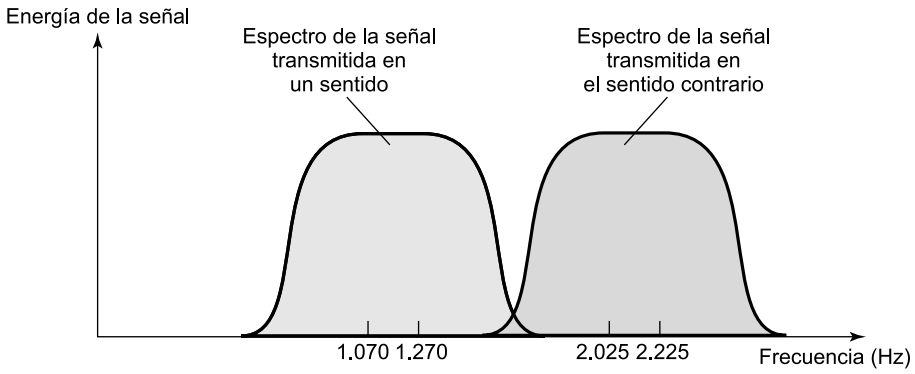

Energía de la señal
Espectro de la señal transmitida en un sentido
Espectro de la señal transmitida en el sentido contrario
1.070 1.270
2.025 2.225
Frecuencia (Hz)

Figura 5.8. Transmisión FSK *full-duplex* en una línea de calidad telefónica.

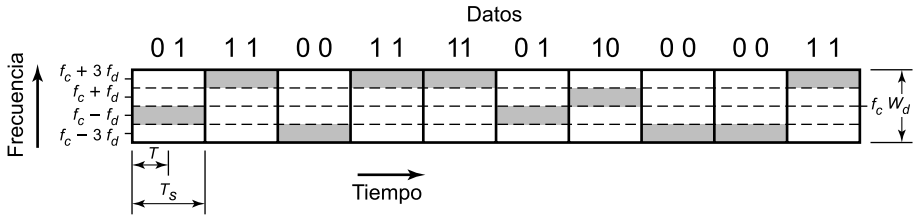


Figura 5.9. Utilización de frecuencias en MFSK ($M = 4$).

Para igualar la velocidad de transmisión de la secuencia de bits a la entrada, cada uno de los elementos de señalización a la salida se genera durante un periodo de $T_s = LT$ segundos, donde T es el periodo correspondiente a la duración de un bit (velocidad de transmisión $= 1/T$). Por tanto, cada elemento de señalización, que en este caso es un tono puro con frecuencia constante, codificará L bits. El ancho de banda necesario es $2Mf_d$. Se puede demostrar que la separación en frecuencia mínima necesaria es $2f_d = 1/T_s$. Por tanto, el modulador requiere un ancho de banda igual a $W_d = 2Mf_d = M/T_s$.

Ejemplo 5.1. Siendo $f_c = 250$ kHz, $f_d = 25$ kHz y $M = 8$ ($L = 3$ bits), para codificar 3 bits se tendrán las siguientes asignaciones de frecuencias para cada una de las 8 posibilidades:

$f_1 = 75$ kHz 000 $f_2 = 125$ kHz 001 $f_3 = 175$ kHz 010 $f_4 = 225$ kHz 011

$f_5 = 275$ kHz 100 $f_6 = 325$ kHz 101 $f_7 = 375$ kHz 110 $f_8 = 425$ kHz 111

Este esquema puede proporcionar una velocidad de transmisión igual a $2f_d = 1/T_s = 50$ kbps.

La Figura 5.9 muestra un ejemplo de MFSK con $M = 4$. Para la secuencia de bits de entrada se codifican 2 bits cada vez, usando una frecuencia distinta para cada una de las cuatro posibles parejas de los bits de entrada.

MODULACIÓN POR DESPLAZAMIENTO DE FASE

En el esquema PSK, la fase de la señal portadora se desplaza para representar los datos digitales.

PSK de dos niveles

En la Figura 5.7c se muestra un ejemplo del sistema más simple, conocido como desplazamiento de fase binario, que utiliza dos fases para representar los dos dígitos binarios. La señal transmitida resultante durante el intervalo correspondiente a un bit es

$$\textbf{BPSK} \qquad s(t) = \begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t + \pi) \end{cases} = \begin{cases} A\cos(2\pi f_c t) & 1 \text{ binario} \\ -A\cos(2\pi f_c t) & 0 \text{ binario} \end{cases} \tag{5.5}$$

El término de la derecha de la Ecuación (5.5) se debe a que un deslazamiento de 180^o (π) es equivalente a invertir la onda sinusoidal, o lo que es lo mismo, a multiplicarla por -1. Esto nos permite utilizar esta expresión más cómoda. Si se dispone de una secuencia de bits y se define $d(t)$ como la función discreta igual a $+1$ durante la duración de un bit si el bit correspondiente en la

secuencia de entrada es 1, e igual a -1 durante la duración de un bit si el bit correspondiente en la secuencia de entrada es 0, entonces, la señal transmitida se puede definir como

$$\textbf{BPSK} \qquad s_d(t) = A\, d(t) \cos(2\pi f_c t) \tag{5.6}$$

Una alternativa a la PSK de dos niveles es la PSK diferencial (DPSK, *Differential PSK*). En la Figura 5.10 se muestra un ejemplo. En este esquema, un 0 binario se representa enviando un elemento de señal con la misma fase que el elemento anterior transmitido. Un 1 binario se representa enviando un elemento de señalización con fase invertida respecto al anterior elemento transmitido. El término *diferencial* se refiere al hecho de que el desplazamiento de fase es respecto al bit transmitido anterior, en lugar de ser respecto a una señal de referencia. En la codificación diferencial, la información a transmitir se representa en términos de los cambios introducidos entre los símbolos consecutivos, en lugar de en los elementos de señalización en sí. DPSK evita la necesidad de utilizar en el receptor un oscilador local de fase preciso, el cual debe estar acoplado con el transmisor. Mientras que la fase anterior se reciba correctamente, la referencia de fase será correcta.

PSK de cuatro niveles

Se puede conseguir un uso más eficaz del ancho de banda si cada elemento de señalización representa más de un bit. Por ejemplo, en lugar de un desplazamiento de fase de 180°, como se hace en BPSK, una técnica habitual de codificación, conocida como modulación por desplazamiento de fase en cuadratura (QPSK, *Quadrature Phase Shift Keying*), considera desplazamientos múltiplos de $\pi/2$ (90°).

$$\textbf{QPSK} \qquad s(t) = \begin{cases} A\cos\left(2\pi f_c t + \dfrac{\pi}{4}\right) & 11 \\ A\cos\left(2\pi f_c t + \dfrac{3\pi}{4}\right) & 01 \\ A\cos\left(2\pi f_c t - \dfrac{3\pi}{4}\right) & 00 \\ A\cos\left(2\pi f_c t - \dfrac{\pi}{4}\right) & 10 \end{cases} \tag{5.7}$$

Por tanto, cada elemento de señalización representa dos bits en lugar de uno.

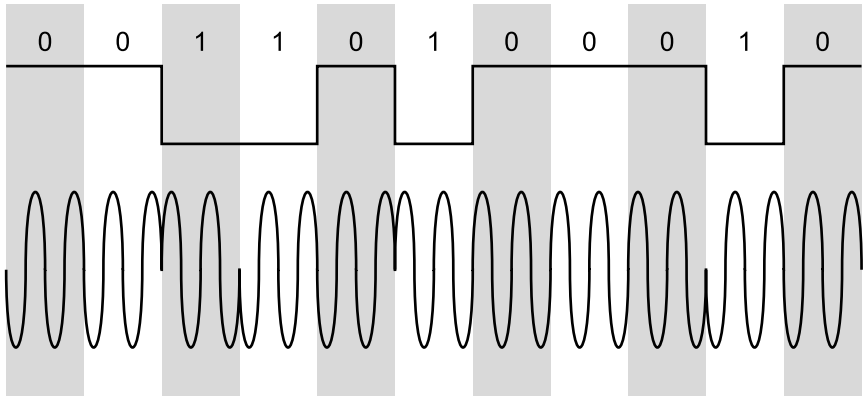


Figura 5.10. Modulación por desplazamiento de fase diferencial (DPSK).

En la Figura 5.11 se muestra un esquema genérico de modulación QPSK. La entrada consiste en una secuencia de dígitos binarios con una velocidad $R = 1/T_b$, siendo T_b la duración de cada bit. Esta secuencia se separa en dos secuencias, cada una de ellas a $R/2$ bps, simplemente asignando un bit alternativamente a cada una de las secuencias. Las dos secuencias se denominan secuencia en fase I (*in-phase*) y secuencia en cuadratura Q (*quadrature phase*). En el diagrama, la secuencia superior se modula con una portadora de frecuencia f_c, multiplicando la secuencia de bits por la portadora. Por cuestiones de comodidad en la estructura del modulador, se hace corresponder el 1 binario con $\sqrt{1/2}$ y el 0 binario con $-\sqrt{1/2}$. Por tanto, un 1 binario se representa mediante una versión escalada de la onda portadora, mientras que un 0 binario se representa mediante una versión escalada y negativa de la onda portadora, ambas con amplitud constante. La misma portadora se desplaza 90° y se utiliza para modular la secuencia binaria inferior. Las dos señales moduladas se suman y se transmiten. La señal transmitida se puede expresar como:

$$\textbf{QPSK} \qquad s(t) = \frac{1}{\sqrt{2}} I(t) \cos 2\pi f_c t - \frac{1}{\sqrt{2}} Q(t) \operatorname{sen} 2\pi f_c t$$

La Figura 5.12 muestra un ejemplo de codificación QPSK. Cada una de las dos secuencias moduladas es una señal BPSK con una velocidad de transmisión igual a la mitad de la de la secuencia de bits original. Por tanto, las señales combinadas tienen una velocidad de símbolos igual a la mitad de la velocidad de los bits a la entrada. Nótese que desde el instante que transcurre entre un símbolo y el siguiente, es factible un cambio de fase de hasta 180° (π).

La Figura 5.11 también muestra una variante de QPSK denominada QPSK desplazada (OQPSK, *offset QPSK*), o también QPSK ortogonal. La diferencia reside en introducir un retardo igual al intervalo de duración de un bit en la secuencia Q, dando lugar a la siguiente señal:

$$s(t) = \frac{1}{\sqrt{2}} I(t) \cos 2\pi f_c t - \frac{1}{\sqrt{2}} Q(t - T_b) \operatorname{sen} 2\pi f_c t$$

Debido a que OQPSK se diferencia de QPSK sólo en el retardo introducido en la secuencia Q, sus características espectrales y sus prestaciones frente a errores son las mismas. A partir de la

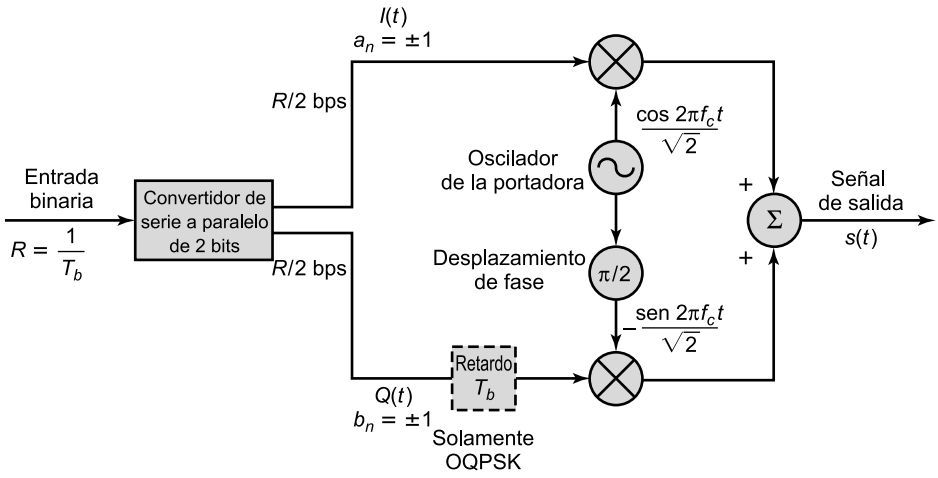


Figura 5.11. Moduladores QPSK y OQPSK.

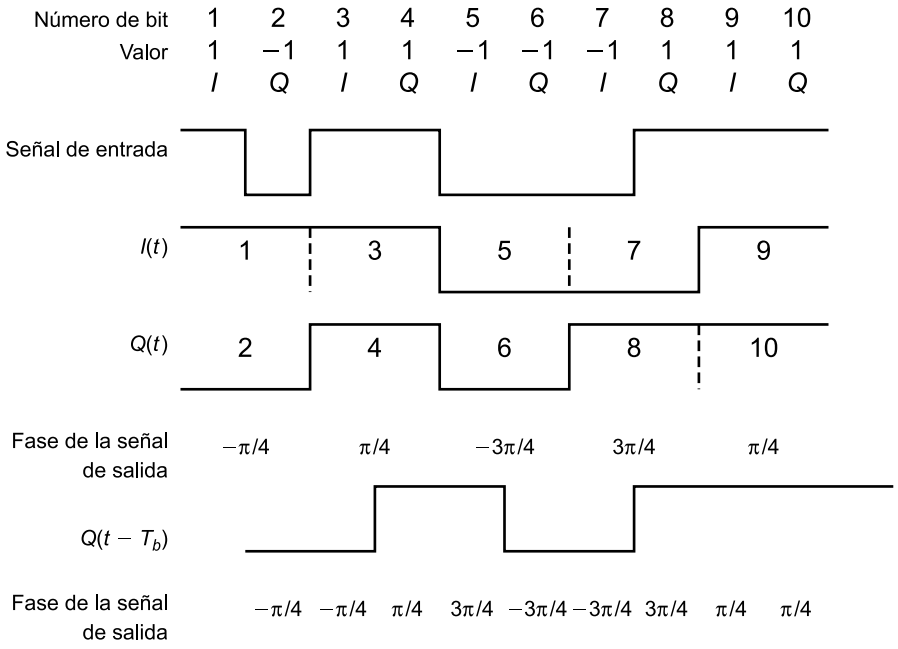

Número de bit 1 2 3 4 5 6 7 8 9 10
Valor 1 −1 1 1 −1 −1 −1 1 1 1
I Q I Q I Q I Q I Q
Señal de entrada
I(t) 1 3 5 7 9
Q(t) 2 4 6 8 10
Fase de la señal de salida −π/4 π/4 −3π/4 3π/4 π/4
Q(t − Tb)
Fase de la señal de salida −π/4 −π/4 π/4 3π/4 −3π/4 −3π/4 3π/4 π/4 π/4

Figura 5.12. Ejemplos de formas de onda en QPSK y OQPSK.

Figura 5.12, se puede observar que sólo uno de los dos bits en el par puede cambiar de signo en cualquier instante de tiempo y, por tanto, el cambio en la fase de la señal combinada nunca sobrepasa los 90^o ($\pi/2$). Esto puede ser una ventaja debido a que las limitaciones físicas en los moduladores de fase hacen que sea difícil conseguir grandes desplazamientos de fase a velocidades de transición altas. OQPSK también proporciona mejores prestaciones cuando el canal de transmisión (incluyendo al transmisor y el receptor) tiene componentes no lineales significativas. El efecto de las no linealidades ensancha el ancho de banda de la señal, lo que puede causar interferencias con canales adyacentes. Si los cambios de fase son menores es más fácil controlar este ensanchamiento; de ahí la ventaja de OQPSK sobre QPSK.

PSK multinivel

La utilización de varios niveles se puede extender para transmitir más de dos bits de una vez. Por ejemplo, usando ocho ángulos de fase diferentes es posible transmitir de una vez tres bits. Es más, cada ángulo puede tener más de una amplitud. Por ejemplo, un módem estándar a 9.600 bps utiliza 12 ángulos de fase, cuatro de los cuales tienen dos valores de amplitud, dando lugar a 16 elementos de señalización diferentes.

Este último ejemplo pone de manifiesto la diferencia entre velocidad de transmisión R (en bps) y velocidad de modulación D (en baudios) de la señal. Supongamos que este sistema se empleara sobre una señal digital en la que cada bit se representara por un pulso constante de tensión, tomando un nivel para el uno binario y otro nivel distinto para el cero. La velocidad de transmisión sería $R = 1/T_b$. Sin embargo, la señal codificada contendrá $L = 4$ bits por cada elemento de señalización, utilizando $M = 16$ combinaciones distintas de amplitud y fase. La velocidad de modulación, en este caso, es $R/4$, ya que cada elemento de señal transporta cuatro bits. Por tanto, la velocidad

de señalización es 2.400 baudios, pero la velocidad de transmisión es igual a 9.600 bps. Esta misma aproximación posibilita mayores velocidades de transmisión en líneas de calidad telefónica mediante la utilización de esquemas de modulación más complejos.

PRESTACIONES

El primer parámetro que se debe considerar para comparar las prestaciones de los distintos esquemas de modulación digital a analógico es el ancho de banda de la señal modulada. Éste dependerá de diversos factores, entre otros, de la propia definición que se haga de ancho de banda, así como de la técnica de filtrado que se use para obtener la señal paso banda. Aquí se utilizarán los resultados obtenidos en [COUC01].

El ancho de banda B_T para ASK es de la forma

$$\textbf{ASK} \qquad B_T = (1 + r)R \tag{5.8}$$

donde R es la velocidad de transmisión y r está relacionada con la técnica de filtrado aplicada para limitar el ancho de banda de la señal, permitiendo así su posterior transmisión. Generalmente, se verifica que $0 < r < 1$. Así, el ancho de banda está directamente relacionado con la velocidad de transmisión. La expresión anterior es también válida para PSK.

Para FSK, el ancho de banda se puede expresar como

$$\textbf{FSK} \qquad B_T = 2\Delta F + (1 + r)R \tag{5.9}$$

donde $\Delta F = f_2 - f_c = f_c - f_1$ es el desplazamiento de la frecuencia de la señal modulada respecto de la frecuencia de la portadora. Cuando se usan frecuencias muy altas, el término ΔF es el dominante. Por ejemplo, uno de los estándares que utiliza FSK en redes locales multipunto sobre cable coaxial usa $\Delta F = 1{,}25$ MHz, $f_c = 5$ MHz y $R = 1$ Mbps. En este caso, el término $2\Delta F = 2{,}5$ MHz domina. En el ejemplo mencionado anteriormente del módem Bell 108, $\Delta F = 100$ Hz, $f_c = 1170$ Hz (en un sentido), y $R = 300$ bps. En este caso, domina el término $(1 + r)R$.

Utilizando PSK multinivel (MPSK) se pueden conseguir mejoras significativas en el ancho de banda. En general,

$$\textbf{MPSK} \qquad B_T = \left(\frac{1 + r}{L}\right)R = \left(\frac{1 + r}{\log_2 M}\right)R \tag{5.10}$$

donde L es el número de bits codificados en cada elemento de señalización y M es el número de elementos de señalización diferentes.

Para FSK multinivel (MFSK), se tiene que

$$\textbf{MFSK} \qquad B_T = \left(\frac{(1 + r)M}{\log_2 M}\right)R \tag{5.11}$$

En la Tabla 5.5 se muestra el cociente entre las velocidades de transmisión, R, y el ancho de banda necesario para distintos esquemas de modulación. Este cociente también se denomina **eficiencia del ancho de banda**. Como su nombre indica, este parámetro es una medida de la eficiencia en la utilización del ancho de banda al transmitir los datos. Por tanto, las mejoras introducidas al utilizar un esquema de señalización multinivel son ya evidentes.

Tabla 5.5. Cociente entre las velocidades de transmisión y el ancho de banda para distintos esquemas de codificación digital a analógico.

	$r = 0$	$r = 0{,}5$	$r = 1$
ASK	1,0	0,67	0,5
FSK			
Banda ancha ($\Delta F \gg R$)	~ 0	~ 0	~ 0
Banda estrecha ($\Delta F \approx f_c$)	1,0	0,67	0,5
PSK	1,0	0,67	0,5
Señalización multinivel			
$L = 4$, $b = 2$	2,00	1,33	1,00
$L = 8$, $b = 3$	3,00	2,00	1,50
$L = 16$, $b = 4$	4,00	2,67	2,00
$L = 32$, $b = 5$	5,00	3,33	2,50

Por supuesto, la discusión anterior hace referencia al espectro de la señal de entrada a la línea de transmisión. Observe que todavía no se ha mencionado nada relacionado con la presencia de ruido. En la Figura 5.4 se resumen algunos resultados relevantes basados en ciertas suposiciones relativas a los sistemas de transmisión [COUC01]. Aquí se representa la tasa de errores por bit en función del cociente E_b/N_0, definido en el Capítulo 3. Por supuesto, cuando este cociente aumenta, la tasa de errores disminuye. Es más, DPSK y BPSK mejoran a ASK y a BFSK en, aproximadamente, 3 dB.

La Figura 5.13 muestra la misma información para distintos valores de M para MFSK y MPSK. Hay una diferencia importante. Para MFSK, la probabilidad de error para un valor dado de E_b/N_0 decrece al aumentar M; lo contrario ocurre en MPSK. Por el contrario, si se comparan las Ecuaciones (6.10) y (6.11), la eficiencia del ancho de banda en MFSK decrece al aumentar M, siendo lo contrario cierto para el esquema MPSK.

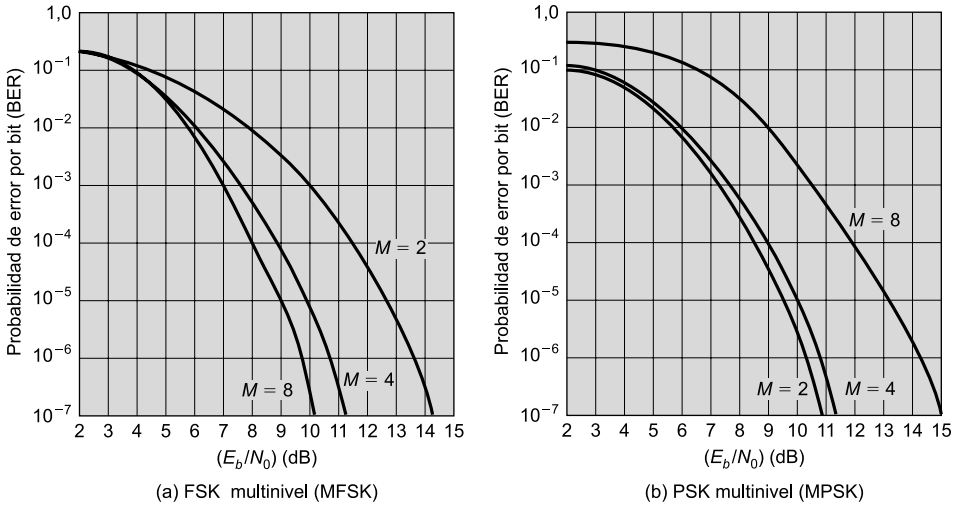


Figura 5.13. Tasas de error por bit teóricas para los esquemas multinivel MFSK y MPSK.

Ejemplo 5.2. ¿Cuál es la eficiencia del ancho de banda en FSK, ASK, PSK y QPSK, siendo la tasa de errores por bit igual a 10^{-7} en un canal con una SNR de 12 dB?

Utilizando la Ecuación (2.2), se tiene que

$$\frac{E_b}{N_0} = 12 \text{ dB} - \left(\frac{R}{B_T}\right)_{\text{dB}}$$

Para FSK y ASK, a partir de la Figura 5.4:

$$\frac{E_b}{N_0} = 14{,}2 \text{ dB}$$

$$\left(\frac{R}{B_T}\right)_{\text{dB}} = -2{,}2 \text{ dB}$$

$$\frac{R}{B_T} = 0{,}6$$

Para PSK, a partir de la Figura 5.4:

$$\frac{E_b}{N_0} = 11{,}2 \text{ dB}$$

$$\left(\frac{R}{B_T}\right)_{\text{dB}} = 0{,}8 \text{ dB}$$

$$\frac{R}{B_T} = 1{,}2$$

En QPSK se debe tener en cuenta que la velocidad de modulación debe verificar que $D = R/2$. Por tanto,

$$\frac{R}{B_T} = 2{,}4$$

Como se muestra en el ejemplo anterior, los esquemas ASK y FSK proporcionan la misma eficiencia del ancho de banda; PSK es mejor y se consigue todavía mayor eficiencia si se utiliza una señalización multinivel.

Es conveniente hacer una comparación de estas necesidades de ancho de banda con las correspondientes a la señalización digital. Una buena aproximación es

$$B_T = 0{,}5(1 + r)D$$

donde D es la velocidad de modulación. En NRZ se cumple que $D = R$, luego

$$\frac{R}{B_T} = \frac{2}{1 + r}$$

Por tanto, la señalización digital es comparable en cuanto a la eficiencia del ancho de banda con ASK, FSK y PSK. Se puede observar una mejora significativa en la señalización analógica al utilizar técnicas multinivel.

MODULACIÓN DE AMPLITUD EN CUADRATURA

La modulación de amplitud en cuadratura (QAM, *Quadrature Amplitude Modulation*) es una técnica de señalización analógica que se utiliza en algunas normas inalámbricas y en las líneas de abonado digitales asimétricas (ADSL, *Asymmetric Digital Subscriber Line*); ambas tecnologías serán explicadas en el Capítulo 8. Esta técnica de modulación es una combinación de ASK y PSK. También se puede considerar como una generalización de QPSK. En QAM se aprovecha el hecho de que es posible enviar simultáneamente dos señales diferentes sobre la misma frecuencia portadora, utilizando dos réplicas de la misma, desplazadas entre sí 90°. En QAM cada portadora se modula usando ASK. Las dos señales independientes se transmiten sobre el mismo medio. En el receptor, las dos señales se demodulan, combinándose para reproducir la señal binaria de entrada.

En la Figura 5.14 se muestra, en términos generales, el esquema de modulación QAM. La entrada al sistema es una cadena de bits con velocidad igual a R bps. Esta cadena se separa en dos secuencias a $R/2$ bps cada una, tomando los bits de forma alternante. En el diagrama, la secuencia de arriba se modula mediante ASK sobre una portadora de frecuencia f_c; este procedimiento se lleva a cabo sin más que multiplicar la secuencia por la portadora. Por tanto, un cero binario será representado mediante la ausencia de portadora, mientras que un uno binario se representará mediante la presencia de una señal portadora de amplitud constante. Esta misma portadora se desplaza 90° y, a su vez, se usa para la modulación ASK de la secuencia binaria de abajo. Las dos señales moduladas se suman y, posteriormente, se transmiten. La señal transmitida, por tanto, se puede expresar como

$$\textbf{QAM} \qquad s(t) = d_1(t)\cos 2\pi f_c t + d_2(t)\,\text{sen}\,2\pi f_c t$$

Si se utiliza un esquema ASK con dos niveles, entonces, cada una de las dos secuencias binarias se podrá representar mediante dos estados, que combinadas dan lugar a una señal con 4 (2×2) posibles estados de señalización. Esto es, esencialmente QPSK. Si se usa ASK con cuatro niveles

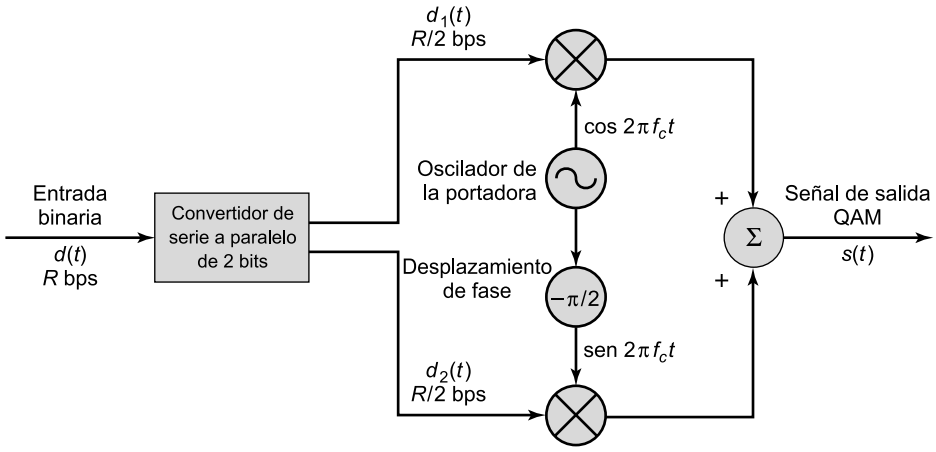


Figura 5.14. Modulador QAM.

(esto es, cuatro niveles diferentes de amplitud), entonces, la secuencia combinada podrá tomar uno de entre 16 (4 × 4) estados. En la práctica, se implementan sistemas con 64, e incluso, 256 estados. Para un ancho de banda dado, cuanto mayor sea el número de estados, mayor será la velocidad de transmisión posible. Desde luego, como ya se ha comentado previamente, cuanto mayor sea el número de estados, mayor será la tasa potencial de errores por bit debida al ruido y a la atenuación.

5.3. DATOS ANALÓGICOS, SEÑALES DIGITALES

En esta sección se estudia el proceso de la transformación de datos analógicos en señales digitales. Estrictamente hablando, es más correcto referirse a este proceso como la conversión de datos analógicos a datos digitales; este proceso es también denominado digitalización. Una vez que los datos analógicos se convierten a digitales puede ocurrir una serie de cosas; de entre ellas, las tres más habituales son las siguientes:

1. Los datos digitales se transmiten usando NRZ-L. En este caso, se habrá realizado directamente una conversión de datos analógicos a señales digitales.
2. Los datos digitales se codifican usando un código diferente al NRZ-L. Por tanto, en este caso se necesitaría un paso adicional.
3. Los datos digitales se convierten en señales analógicas, usando una de las técnicas de modulación presentadas en la Sección 5.2.

Este último procedimiento, aparentemente curioso, se muestra en la Figura 5.15, en la que se representan algunos datos de voz digitalizados, los cuales son posteriormente convertidos en señales analógicas tipo ASK. Este procedimiento permite la transmisión digital, en el mismo sentido que la definición del Capítulo 3. Los datos de voz, al haber sido digitalizados, se pueden procesar como si fueran digitales, incluso cuando los requisitos de la transmisión (por ejemplo, al usar microondas) fuercen la utilización de señales analógicas.

El dispositivo que se utiliza para la conversión de los datos analógicos en digitales y que, posteriormente, recupera los datos analógicos iniciales a partir de los digitales se denomina *codec* (codificador-decodificador). En esta sección se estudiarán las dos técnicas más importantes usadas en los *codec*, es decir, la modulación por impulsos codificados y la modulación delta. La sección concluye comparando sus prestaciones.

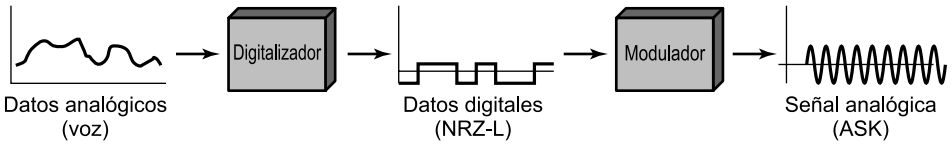


Figura 5.15. Digitalización de datos analógicos.

MODULACIÓN POR IMPULSOS CODIFICADOS

La modulación por impulsos codificados (PCM, *Pulse Code Modulation*) se basa en el teorema de muestreo:

Teorema de muestreo. Si una señal $f(t)$ se muestrea a intervalos regulares de tiempo con una frecuencia mayor que el doble de la frecuencia más alta de la señal, las muestras así obtenidas contienen toda la información de la señal original. La función $f(t)$ se puede reconstruir a partir de estas muestras mediante la utilización de un filtro paso baja.

Para el lector interesado, en el sitio web asociado a este texto se proporciona la demostración del teorema anterior. Si los datos de voz se limitan a frecuencias por debajo de 4000 Hz, lo que significa que la inteligibilidad se conserva, para caracterizar completamente la señal de voz sería suficiente obtener 8000 muestras por segundo. Obsérvese que aún se trata de muestras analógicas, denominadas muestras de **modulación por impulsos de amplitud** (PAM, *Pulse Amplitude Modulation*). Para convertir las muestras PAM a digital, a cada una de ellas se les debe asignar un código binario.

En la Figura 5.16 se muestra un ejemplo en el que se supone que la señal original está limitada en banda, siendo B el ancho de banda. Las muestras PAM se toman a una tasa igual a $2B$, o lo que es lo mismo, una vez cada $T_s = 1/2B$ segundos. Cada muestra PAM se aproxima mediante su *cuantización* en uno de los 16 posibles niveles. Por tanto, cada una de las muestras se puede representar por 4 bits. Sin embargo, debido a que los niveles cuantizados son sólo aproximaciones, es imposible recuperar la señal original con exactitud. Utilizando muestras de 8 bits, lo que permite 256 niveles de cuantización, la calidad de la señal de voz resultante es comparable a la que se consigue mediante transmisión analógica. Nótese que esto implica que para una única señal de voz se necesitan 8.000 muestras por segundo × 8 bits por muestra = 64 kbps.

Así pues, la técnica PCM genera la señal digital tomando como entrada la señal analógica continua en el tiempo y en amplitud (*véase* Figura 5.17). La señal digital resultante consiste en bloques de n bits, donde cada número de n bits corresponde con la amplitud de un impulso PCM. En el receptor, este procedimiento se invierte para obtener así la señal analógica. Obsérvese, no

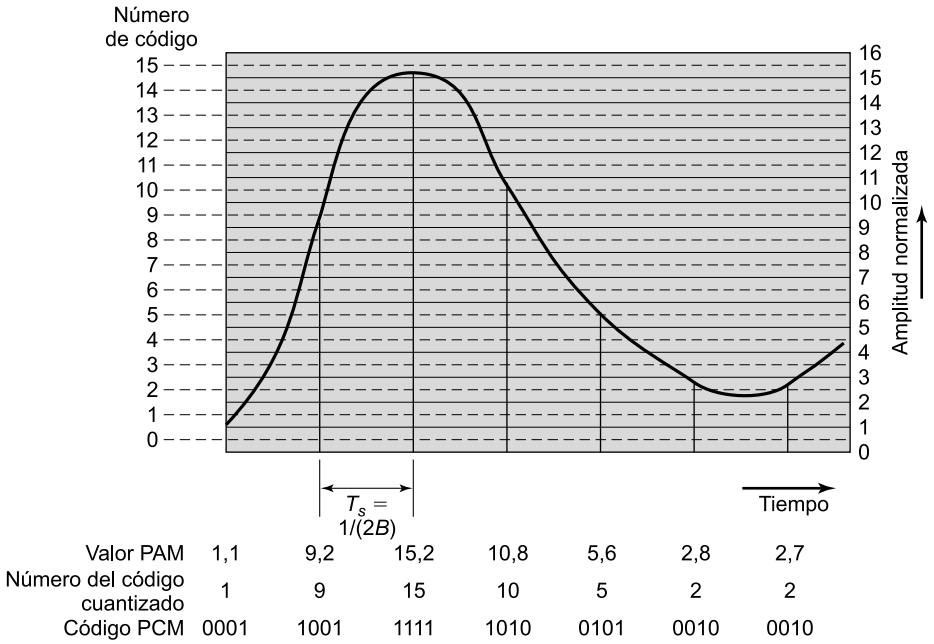


Figura 5.16. Ejemplo de modulación por impulsos codificados.

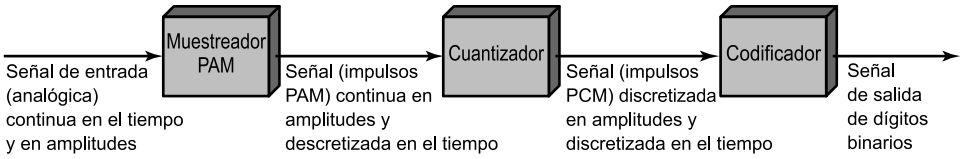

Señal de entrada (analógica) continua en el tiempo y en amplitudes
Muestreador PAM
Señal (impulsos PAM) continua en amplitudes y descretizada en el tiempo
Cuantizador
Señal (impulsos PCM) discretizada en amplitudes y discretizada en el tiempo
Codificador
Señal de salida de dígitos binarios

Figura 5.17. Diagrama de bloques del esquema PCM.

obstante, que este proceso viola las condiciones exigidas por el teorema de muestreo. Al cuantizar los impulsos PAM, la señal original sólo se aproxima, por lo que no podrá ser recuperada con exactitud. Este efecto se denomina error de cuantización o ruido de cuantización. La razón señal-ruido para el ruido de cuantización se puede expresar como [GIBS93]:

$$\text{SNR}_{\text{dB}} = 20 \log 2^n + 1{,}76 \text{ dB} = 6{,}02n + 1{,}76 \text{ dB}$$

Por tanto, en la cuantización, cada bit adicional que se use aumentará la SNR en 6 dB, lo que es igual a un factor 4.

Generalmente, el esquema PCM se refina mediante técnicas denominadas de codificación no lineal, en las que los niveles de cuantización no están igualmente separados. El problema que surge al considerar separaciones entre niveles iguales es que el valor medio del valor absoluto del error, para cada muestra, es el mismo, independientemente del nivel de la señal. Por consiguiente, los niveles de señal más pequeños estarán, en términos relativos, más distorsionados. Al usar un número mayor de niveles de cuantización para señales de poca amplitud y un número menor para las señales de mayor amplitud se consigue una reducción en la distorsión media de la señal (por ejemplo, *véase* la Figura 5.18).

El mismo efecto se puede conseguir usando cuantización uniforme, pero comprimiendo y, posteriormente, expandiendo la señal analógica de entrada. Este procedimiento consiste en comprimir a la entrada el rango de intensidades de la señal, asignando a las señales de baja amplitud una ganancia superior que a las señales de amplitud mayor. En la salida se realiza la operación contraria. En la Figura 5.19 se representa una función típica de compresión-expansión. Nótese que el

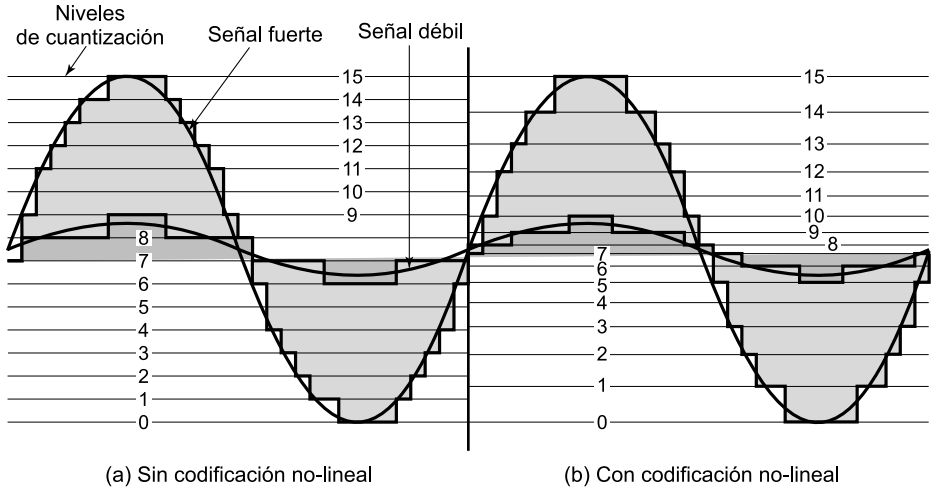


Figura 5.18. Efecto de la codificación no-lineal.

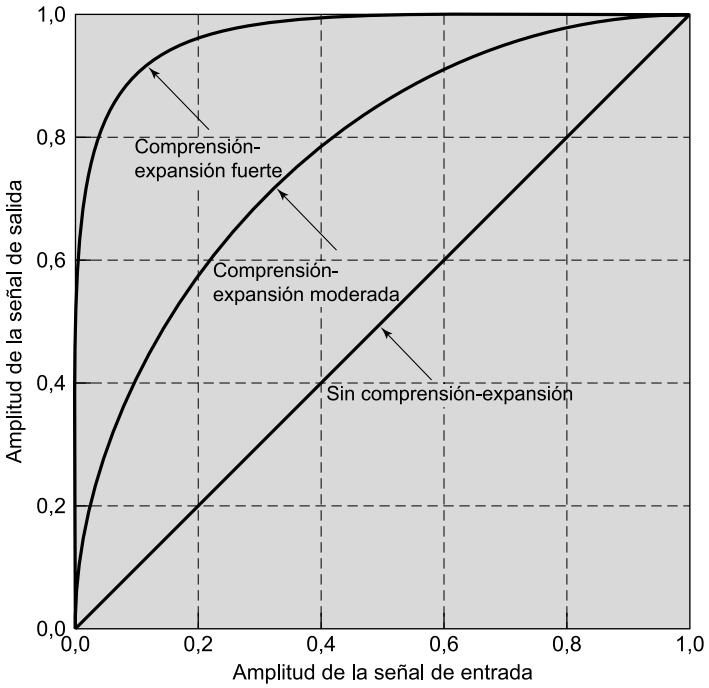


Figura 5.19. Funciones típicas de compresión-expansión.

efecto en la entrada es comprimir las muestras de forma tal que los valores grandes se reducen con respecto a los valores pequeños. Por tanto, teniendo un número fijo de niveles de cuantización, se dispondrá de más niveles para las señales de menor nivel. A la salida, la compresión-expansión expande las muestras de forma tal que se restauran los valores originales.

En un sistema PCM la codificación no lineal puede conseguir una mejora significativa de la SNR. Para las señales de voz se han conseguido mejoras de 24 a 30 dB.

MODULACIÓN DELTA

Para mejorar las prestaciones de la codificación PCM, o para reducir su complejidad, se han desarrollado un gran número de técnicas. Una de las alternativas de mayor aceptación es la modulación delta (DM, *Delta Modulation*).

En la modulación delta, la entrada analógica se aproxima mediante una función escalera que en cada intervalo de muestreo (T_s) sube o baja un nivel de cuantización (δ). En la Figura 5.20 se muestra un ejemplo, en el que la función escalera está superpuesta a la señal original. La característica principal de la función escalera es que su comportamiento es binario: en cada instante de muestreo la función sube o baja una cantidad constante δ. Por tanto, la salida del modulador delta se puede representar mediante un único bit para cada muestra. Resumiendo, en lugar de aproximar a las amplitudes, DM obtiene una cadena de bits que aproxima a la derivada de la señal analógica de entrada: se genera un 1 si la función escalera sube en el siguiente intervalo o un 0, en cualquier otro caso.

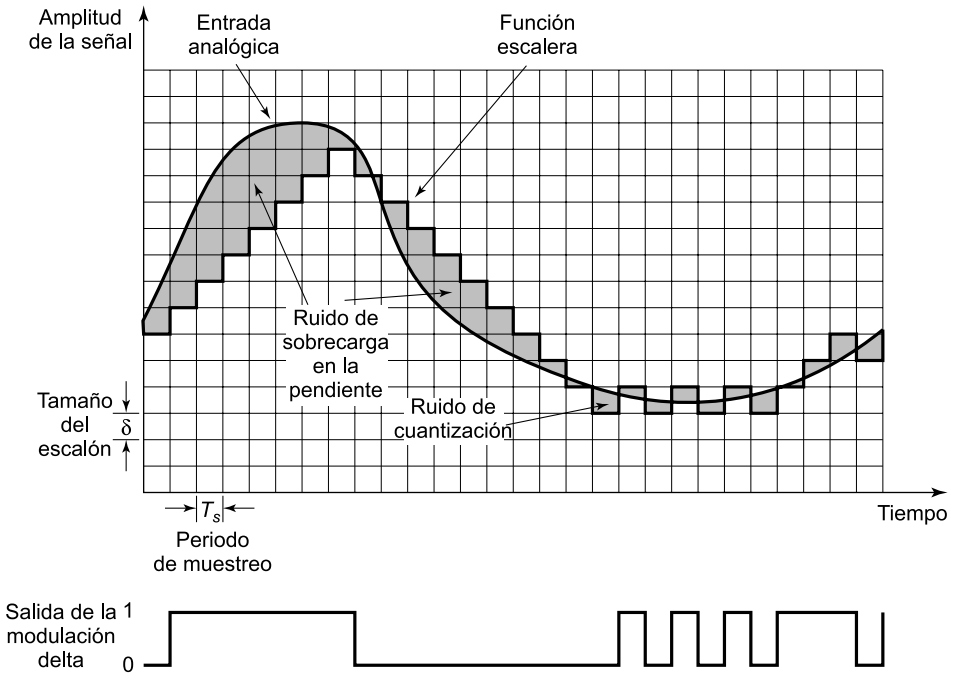


Figura 5.20. Ejemplo de modulación delta.

La transición (hacia arriba o hacia abajo) que ocurre en cada intervalo de muestreo se elige de tal manera que la función escalera se aproxime tanto como sea posible a la forma de onda de la señal original. La Figura 5.21 muestra este procedimiento, que básicamente consiste en un mecanismo de realimentación. Al transmitir ocurre lo siguiente: para cada intervalo de muestreo, la señal analógica de entrada se compara con el valor más reciente de la función escalera. Si el valor de la forma de onda muestreada supera el de la función escalera, se genera un 1; en otro caso, se generará un 0. Por tanto, la función escalera siempre se modifica en la dirección de la señal de entrada. La salida del proceso DM es, por tanto, una secuencia binaria que se puede usar en el receptor para reconstruir la función escalera. La función reconstruida se podrá suavizar mediante algún procedimiento de integración o mediante un filtro paso baja que genere una aproximación analógica a la señal de entrada.

Hay dos parámetros importantes en el esquema DM: el tamaño del paso asignado a cada dígito binario, δ, y la frecuencia de muestreo. Como se muestra en la Figura 5.20, δ se debe elegir de forma que se consiga un compromiso entre dos tipos de error o ruidos. Cuando la señal analógica varíe muy lentamente, habrá ruido de cuantización, siendo este ruido tanto mayor cuanto mayor sea δ. Por el contrario, cuando la señal de entrada cambie tan rápidamente que la función escalera no la pueda seguir, se producirá un ruido de sobrecarga en la pendiente. Este ruido aumenta al disminuir δ.

Debe quedar claro que la precisión de este esquema se puede mejorar aumentando la frecuencia de muestreo. No obstante, esto incrementará la velocidad de transmisión de los datos a la salida.

La principal ventaja de DM respecto a PCM es su sencillez de implementación. No obstante, PCM consigue en general una mejor SNR para la misma velocidad de transmisión.

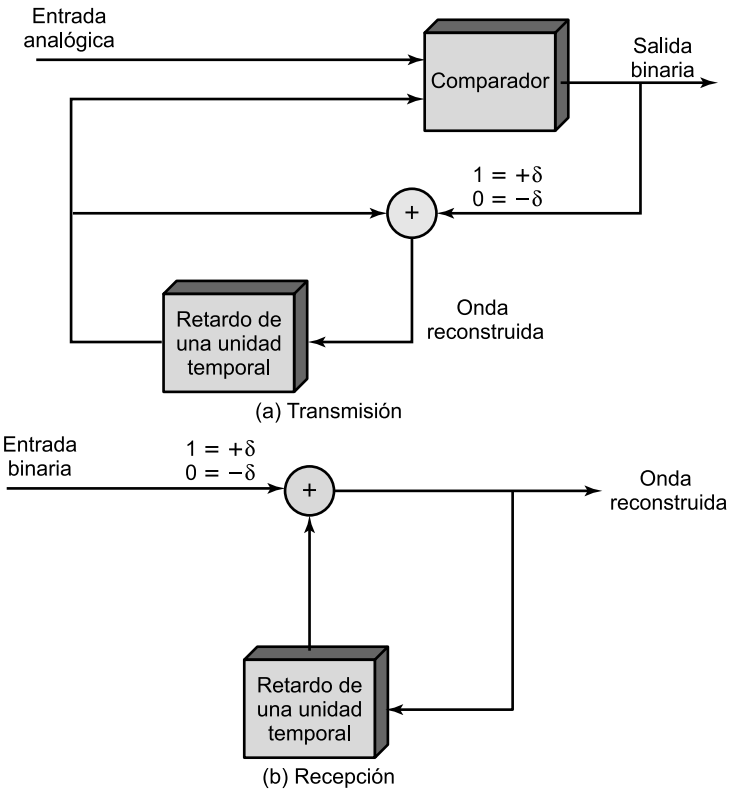


Figura 5.21. Modulación delta.

PRESTACIONES

Se puede conseguir una buena calidad de reproducción de voz con 128 niveles en PCM, es decir, con 7 bits ($2^7 = 128$). La señal de voz, siendo conservador, ocupa un ancho de banda de 4 kHz. Por tanto, de acuerdo con el teorema de muestreo, las muestras se pueden tomar a una razón de 8.000 muestras por segundo. Esto implica que, para los datos digitales codificados en PCM, se obtiene una velocidad de transmisión igual a $8.000 \times 7 = 56$ kbps.

Veamos qué implicaciones tiene esto desde el punto de vista del ancho de banda necesario. Una señal analógica de voz ocupa 4 kHz. Esta señal analógica de 4 kHz se convierte mediante PCM en una señal digital a 56 kbps. De acuerdo con el criterio de Nyquist (*véase* Capítulo 3) esta señal digital necesitaría aproximadamente 28 kHz de ancho de banda. Este hecho será tanto más evidente cuanto mayor sea el ancho de banda de la señal considerada. Por ejemplo, un esquema típico PCM para televisión en color de 4,6 MHz de ancho de banda utiliza códigos de 10 bits, que se transmiten a 92 Mbps. A pesar de lo elevado de estas cifras, las técnicas de transmisión digital se utilizan cada vez más en la transmisión de datos analógicos. Este hecho está justificado por las siguientes razones:

- Debido a que se usan repetidores en lugar de amplificadores, no hay ruido aditivo.
- Como se verá posteriormente, para señales digitales, en lugar de utilizar multiplexación por división en frecuencias (FDM, *Frecuency-Division Multiplexing*) se usa la multiplexación

por división en el tiempo (TDM, *Time-Division Multiplexing*). En TDM no hay ruido de intermodulación, aunque, como ya se ha visto, sí que está presente en FDM.

- La conversión a señales digitales permite el uso de técnicas más eficaces de conmutación.

Es más, se han desarrollando técnicas que proporcionan códigos más eficaces. Para el caso de la voz, un objetivo que parece razonable está en torno a 4 kbps. Para la codificación de señales de vídeo, se puede usar el hecho de que la mayor parte de los elementos de la imagen no cambian cuadro a cuadro. Las técnicas de codificación que aprovechan las dependencias existentes entre cuadros consecutivos permiten reducir la velocidad de transmisión para la señal de vídeo hasta 15 Mbps y, para secuencias que varíen poco, por ejemplo una tele-conferencia, se puede reducir hasta 64 kbps, o incluso menos.

Finalmente, hay que decir que, en muchos casos, el uso de un sistema de telecomunicación dará lugar tanto a una conversión de digital a analógico como a una de analógico a digital. La mayoría de los terminales en las redes de telecomunicación son analógicos y las redes utilizan una mezcla de técnicas y dispositivos analógicos y digitales. Por tanto, los datos digitales en el terminal del usuario se deberán convertir a analógico mediante un módem, posteriormente, se deberán digitalizar mediante un *codec* y, posiblemente, todavía sufran conversiones adicionales antes de alcanzar su destino final.

Debido a esto, los servicios de telecomunicación gestionan señales analógicas que representan tanto voz como datos digitales. Las características de la forma de las ondas respectivas son bastante diferentes. Mientras que las señales de voz tienden a estar concentradas en la parte baja del ancho de banda (*véase* Figura 3.9), la codificación analógica de señales digitales tiene una distribución espectral más uniforme, conteniendo, por tanto, más componentes a altas frecuencias. Algunos estudios han demostrado que, debido a la presencia de estas frecuencias altas, en la digitalización de señales analógicas que representan datos digitales, es preferible el uso de técnicas tipo PCM, en lugar de optar por procedimientos similares a DM.

5.4. DATOS ANALÓGICOS, SEÑALES ANALÓGICAS

La modulación se ha definido como el proceso de combinar una señal de entrada $m(t)$ y una portadora a frecuencia f_c para producir una señal $s(t)$ cuyo ancho de banda esté (normalmente) centrado en torno a f_c. Para el caso de datos digitales, la justificación de la modulación es evidente: será necesaria cuando sólo exista la posibilidad de transmisión analógica, permitiendo así convertir los datos digitales en analógicos. Sin embargo, cuando los datos son analógicos, la justificación no es tan evidente. Después de todo, las señales de voz se transmiten a través de líneas telefónicas usando su espectro original (esto se denomina transmisión en banda base). Existen dos razones fundamentales para la transmisión de señales analógicas mediante modulación analógica:

- Para llevar a cabo una transmisión más efectiva puede que se necesite una frecuencia mayor. En los medios no guiados es prácticamente imposible transmitir señales en banda base, ya que el tamaño de las antenas tendría que ser de varios kilómetros de diámetro.
- La modulación permite la multiplexación por división en frecuencias, técnica muy importante que se estudiará en el Capítulo 8.

En esta sección consideraremos las técnicas más importantes para la modulación de datos analógicos: la modulación de amplitud (AM, *Amplitude Modulation*), la modulación de frecuencia (FM, *Frecuency Modulation*) y la modulación de fase (PM, *Phase Modulation*). Al igual que antes, para llevar a cabo la modulación se utilizan los tres parámetros básicos de la portadora.

MODULACIÓN DE AMPLITUD

La modulación de amplitud (AM), mostrada en la Figura 5.22, es la técnica más sencilla de modulación. Matemáticamente, el proceso se puede expresar como

$$\textbf{AM} \qquad s(t) = [1 + n_a x(t)] \cos 2\pi f_c t \tag{5.12}$$

donde $\cos 2\pi f_c t$ es la portadora y $x(t)$ es la señal de entrada (los datos), ambas normalizadas a la amplitud unidad. El parámetro n_a, denominado **índice de modulación**, es el cociente entre la amplitud de la señal de entrada y la amplitud de la portadora. De acuerdo con la notación previa, la señal de entrada será $m(t) = n_a x(t)$. El «1» en la Ecuación (5.12) es una componente continua que, como se explica a continuación, evita pérdidas de información. Este esquema también se denomina transmisión en doble banda lateral con portadora (DSBTC, *Double Sideband Transmitted Carrier*).

Ejemplo 5.3. Obtener la expresión de $s(t)$, si $x(t)$, la señal moduladora en amplitud es $\cos 2\pi f_m t$. Se tiene que

$$s(t) = [1 + n_a \cos 2\pi f_m t] \cos 2\pi f_c t$$

Utilizando identidades trigonométricas, la expresión anterior se puede desarrollar, obteniéndose

$$s(t) = \cos 2\pi f_c t + \frac{n_a}{2} \cos 2\pi (f_c - f_m) t + \frac{n_a}{2} \cos 2\pi (f_c + f_m) t$$

La señal resultante tiene una componente a la frecuencia original de la portadora, más un par de componentes adicionales separadas f_m hercios de la frecuencia de la portadora.

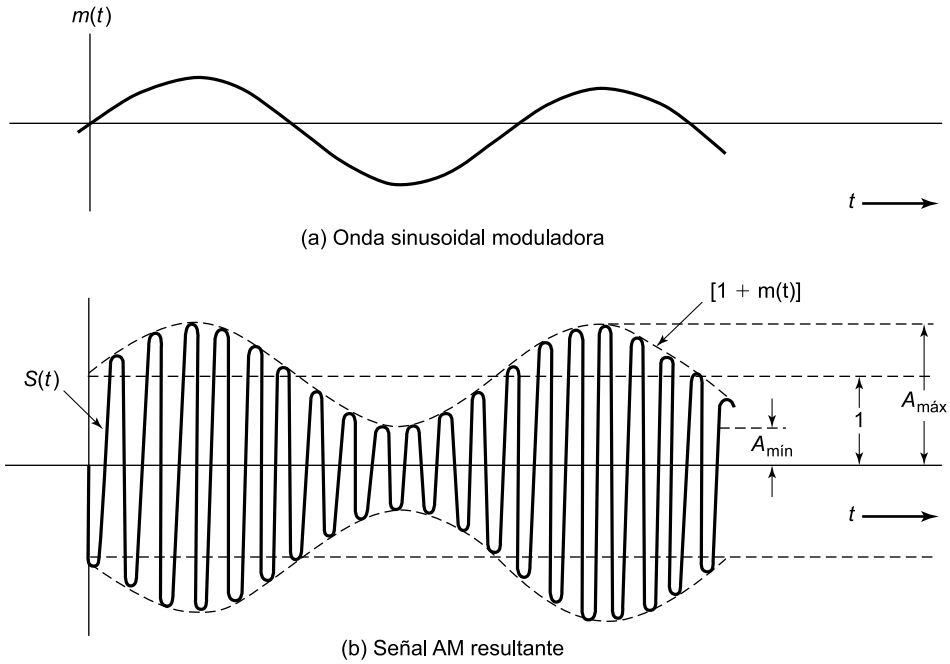


Figura 5.22. Modulación de amplitud.

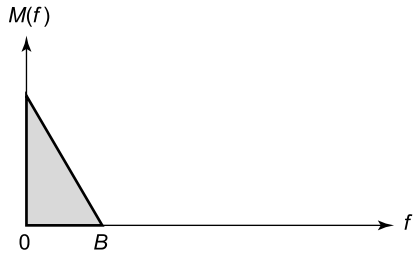
A partir de la expresión (5.12) y de la Figura 5.22, se puede observar que AM implica la multiplicación de la señal de entrada por la portadora. La envolvente de la señal resultante es $[1 + n_a x(t)]$ y, mientras que $n_a < 1$, la envolvente será una reproducción exacta de la señal original. Si $n_a > 1$, la envolvente cruzará el eje de tiempos, perdiéndose así información.

Es instructivo observar el espectro de la señal AM. En la Figura 5.23 se muestra un ejemplo. El espectro está formado por la portadora original más el espectro de la señal de entrada trasladada a f_c. La parte del espectro para la que $|f| > |f_c|$ es la *banda lateral superior* y la porción del espectro para la que $|f| < |f_c|$ es la *banda lateral inferior*. Tanto la banda superior como la inferior son réplicas exactas del espectro original $M(f)$, estando la banda inferior invertida en frecuencias. A modo de ejemplo, considérese la modulación de la señal de voz, con un espectro comprendido entre 300 y 3.000 Hz, sobre una portadora de 60 kHz. La señal resultante estará constituida por la banda superior, entre 60,3 y 63 kHz, y la banda inferior entre 57 y 59,7 kHz, además de la portadora de 60 kHz. Una relación importante es

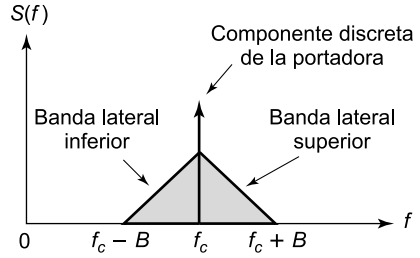
$$P_t = P_c\left(1 + \frac{n_a^2}{2}\right)$$

donde P_t es la potencia total transmitida en $s(t)$ y P_c es la potencia transmitida en la portadora. Es deseable hacer n_a tan grande como sea posible, de tal manera que la mayor parte de la potencia de la señal transmitida se use para transportar información. Ahora bien, n_a debe mantenerse menor que 1.

Debería estar claro que $s(t)$ contiene componentes innecesarias, ya que cada una de las bandas laterales contiene todo el espectro de $m(t)$. Una variante de AM, denominada AM de banda lateral única (SSB, *Single Sideband*), aprovecha este hecho transmitiendo sólo una de las bandas laterales, eliminando la otra y la portadora. Las principales ventajas de esta aproximación son:



(a) Espectro de la señal moduladora



(b) Espectro de una señal AM con portadora a f_c

Figura 5.23. Espectro de una señal AM.

- Sólo se necesita la mitad del ancho de banda, es decir $B_T = B$, donde B es el ancho de banda de la señal original. En DSBTC, $B_T = 2B$.
- Se necesita menos potencia, ya que se ahorra la potencia correspondiente a la portadora y a la otra banda lateral. Otra variante es la doble banda lateral con portadora suprimida (DSBSC, *Double Sideband Supressed Carrier*), en la que se filtra la frecuencia portadora y se transmiten las dos bandas laterales. Con este procedimiento se ahorra algo de potencia, pero se utiliza igual ancho de banda que en DSBTC.

La desventaja de suprimir la portadora es que dicha componente se puede usar para la sincronización. Por ejemplo, supóngase que la señal analógica original es una forma de onda ASK que codifica datos digitales. El receptor necesitará conocer dónde comienza cada bit, para así interpretar correctamente los datos. Una portadora constante proporciona un mecanismo de sincronización con el que se puede temporizar la llegada de los bits. Una aproximación que implica un compromiso es la denominada banda lateral residual (VSB, *Vestigial Sideband*), en la que se usa una de las bandas laterales y una portadora de potencia reducida.

MODULACIÓN ANGULAR

La modulación de frecuencia (FM) y la modulación de fase (PM) son casos particulares de la denominada modulación angular. La señal modulada se expresa como

$$\textbf{Modulación angular} \qquad s(t) = A_c \cos\left[2\pi f_c t + \phi(t)\right] \tag{5.13}$$

En la modulación de fase, la fase es proporcional a la señal moduladora:

$$\textbf{PM} \qquad \phi(t) = n_p m(t) \tag{5.14}$$

donde n_p es el índice de modulación de fase.

En la modulación de frecuencia, la derivada de la fase es proporcional a la señal moduladora:

$$\textbf{FM} \qquad \phi'(t) = n_f m(t) \tag{5.15}$$

donde n_f es el índice de modulación de frecuencia.

Para el lector que desee una explicación más detallada, sígase la siguiente argumentación matemática. La fase de $s(t)$ en cualquier instante dado es $2\pi f_c t + \phi(t)$. La desviación de la fase instantánea respecto de la señal portadora es $\phi(t)$. En PM, esta desviación instantánea de fase es proporcional a $m(t)$. Debido a que la frecuencia se puede definir como la razón del cambio de fase de una señal, la frecuencia instantánea de $s(t)$ viene dada por

$$2\pi f_i(t) = \frac{d}{dt}\left[2\pi f_c t + \phi(t)\right]$$

$$f_i(t) = f_c + \frac{1}{2\pi}\,\phi'(t)$$

y la desviación de la frecuencia instantánea respecto a la frecuencia de la portadora es $\phi'(t)$, que en FM es proporcional a $m(t)$.

En la Figura 5.24 se muestra la modulación de amplitud, frecuencia y fase de una señal seno. El aspecto de las señales FM y PM es muy parecido. De hecho, es imposible diferenciarlas sin tener un conocimiento previo de la función de modulación.

Respecto a FM, se pueden realizar las siguientes observaciones. La desviación de pico ΔF se puede obtener como

$$\Delta F = \frac{1}{2\pi} n_f A_m \text{ Hz}$$

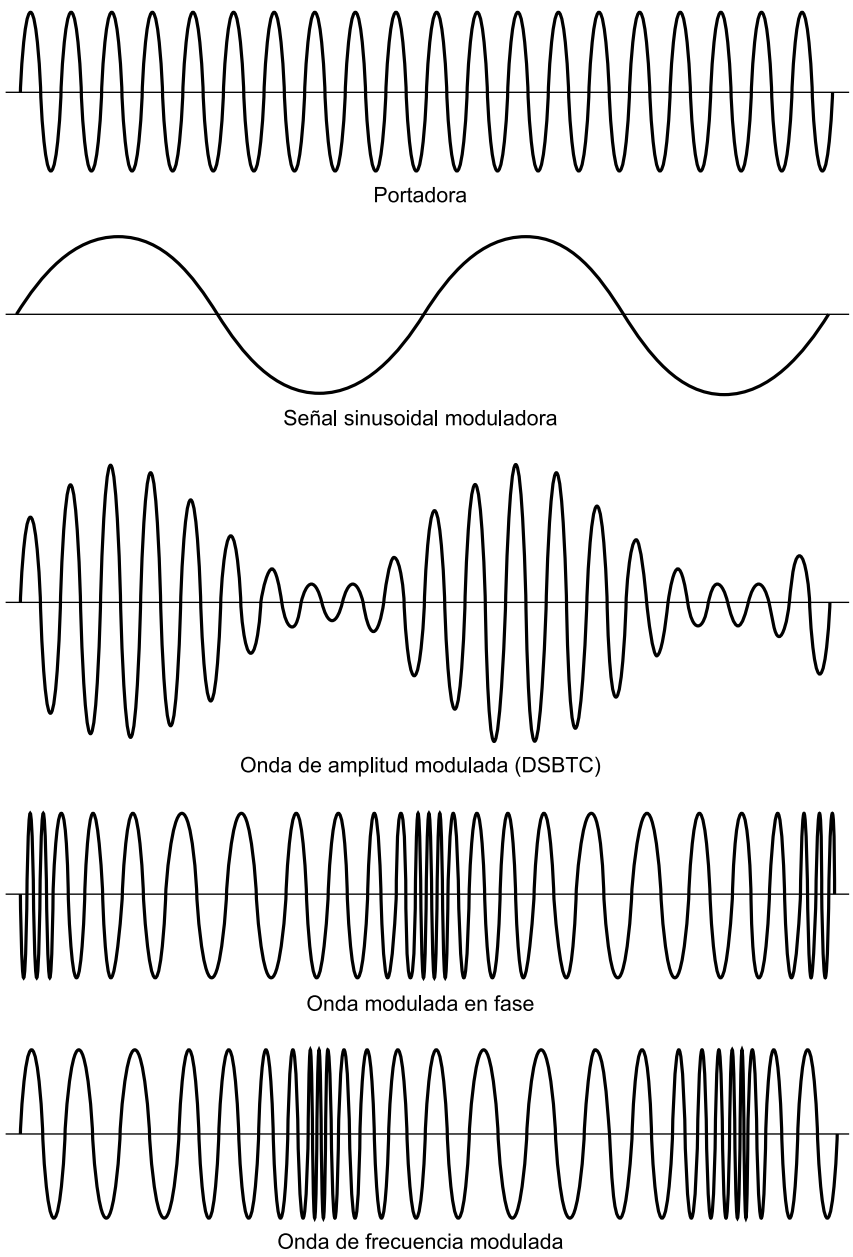


Figura 5.24. Modulación de amplitud, fase y frecuencia de una portadora sinusoidal mediante una señal sinusoidal.

donde A_m es al valor máximo de $m(t)$. Por tanto, un incremento en la amplitud de $m(t)$ aumentará ΔF, lo que, intuitivamente, debería aumentar el ancho de banda transmitido B_T. Sin embargo, como se evidencia a partir de la Figura 5.24, esto no incrementa el nivel de potencia medio de la señal FM, igual a $A_c^2/2$. Esto es diferente a lo que ocurre en AM, ya que el nivel de modulación afecta a la potencia de la señal AM pero no afecta a su ancho de banda.

Ejemplo 5.4. Obtener la expresión de $s(t)$ si $\phi(t)$, la señal modulada en fase, es $n_p \cos 2\pi f_m t$. Supóngase que $A_c = 1$. Entonces, se obtiene directamente que

$$s(t) = \cos [2\pi f_c t + n_p \cos 2\pi f_m t]$$

La desviación intantánea de fase respecto a la señal portadora es $n_p \cos 2\pi f_m t$. El ángulo de fase de la señal varía respecto de su valor no modulado como una señal sinusoidal, siendo el valor de pico de la desviación en fase igual a n_p.

La expresión anterior se puede desarrollar teniendo en cuenta las identidades trigonométricas de Bessel, es decir:

$$s(t) = \sum_{n=-\infty}^{\infty} J_n(n_p) \cos\left(2\pi f_c t + 2\pi n f_m t + \frac{n\pi}{2}\right)$$

donde $J_n(n_p)$ es la n-ésima función de Bessel de primera clase. Teniendo en cuenta que

$$J_{-n}(x) = (-1)^n J_n(x)$$

se puede rescribir como

$$s(t) = J_0(n_p) \cos 2\pi f_c t + \\ + \sum_{n=1}^{\infty} J_n(n_p) \left[\cos\left(2\pi(f_c + n f_m)t + \frac{n\pi}{2}\right) + \cos\left(2\pi(f_c - n f_m)t + \frac{(n+2)\pi}{2}\right)\right]$$

La señal resultante tiene una componente a la frecuencia de la portadora original más un conjunto de bandas laterales desplazadas respecto de f_c por todos los posibles múltiplos de f_m. Para $n_p \ll 1$, los términos de orden superior caen rápidamente.

Ejemplo 5.5. Obtener la expresión de $s(t)$ si $\phi'(t)$, la señal moduladora en frecuencias, es de la forma $-n_f \operatorname{sen} 2\pi f_m t$. La expresión de $\phi'(t)$ se ha elegido por cuestiones de sencillez. Se tiene que

$$\phi(t) = -\int n_f \operatorname{sen} 2\pi f_m t \, dt = \frac{n_f}{2\pi f_m} \cos 2\pi f_m t$$

Por tanto,

$$s(t) = \cos\left[2\pi f_c t + \frac{n_f}{2\pi f_m} \cos 2\pi f_m t\right]$$

$$= \cos\left[2\pi f_c t + \frac{\Delta F}{f_m} \cos 2\pi f_m t\right]$$

La desviación de la frecuencia instantánea respecto de la frecuencia de la portadora es $-n_f \text{sen}\, 2\pi f_m t$. La frecuencia de la señal varía sinusoidalmente en torno a su valor no modulado, siendo la desviación máxima en frecuencias igual a n_f radianes/segundo.

Sustituyendo $\Delta F/f_m$ por n_p, la expresión para la señal FM es idéntica a la correspondiente señal PM, es decir, el desarrollo de Bessel es el mismo.

Al igual que en AM, tanto FM como PM dan lugar a una señal cuyo ancho de banda está centrado en torno a f_c. Sin embargo, a continuación se verá que las magnitudes de sus anchos de banda son muy diferentes. La modulación de amplitud es un proceso lineal que produce frecuencias correspondientes a la suma y a la diferencia de la portadora y de las componentes de la señal moduladora. Por tanto, para AM se tiene que

$$B_T = 2B$$

No obstante, la modulación de ángulo incluye un término de la forma $\cos(\phi(t))$, que evidentemente es no lineal. Este término generará un gran rango de frecuencias. En definitiva, para una señal moduladora sinusoidal de frecuencia f_m, $s(t)$ contendrá componentes en $f_c + f_m$, $f_c + 2f_m$, y así sucesivamente. En el caso más general, para la transmisión de una señal FM o PM se necesitará un ancho de banda infinito. En la práctica, una buena aproximación nemotécnica es la denominada ley de Carson [COUC01], dada por

$$B_T = 2(\beta + 1)B$$

donde

$$\beta = \begin{cases} n_p A_m & \text{para PM} \\ \dfrac{\Delta F}{B} = \dfrac{n_f A_m}{2\pi B} & \text{para FM} \end{cases}$$

La expresión para FM se puede rescribir de la siguiente manera

$$B_T = 2\Delta F + 2B$$

Luego, tanto FM como PM necesitan un ancho de banda mayor que AM.

5.5. LECTURAS RECOMENDADAS

Por diversos motivos, es difícil encontrar manuales que presenten un tratamiento riguroso sobre los esquemas de codificación digital a digital. [SKLA01] y [BERG96] presentan estudios de utilidad.

Por el contrario, hay un gran número de buenas referencias sobre los esquemas de modulación analógica de datos digitales. Una buena elección sería [COUC01], [XION00] y [PROA02]; estos tres también proporcionan un buen tratamiento de la modulación analógica y digital de datos analógicos.

[PEAR92] contiene una exposición excepcionalmente clara que cubre las técnicas de digital a analógico, de analógico a digital y de analógico a analógico.

[FREE98] es un texto instructivo que abarca conceptos como la velocidad de transmisión, la velocidad de modulación y el ancho de banda. [SKLA93] es un tutorial recomendable que explica más ampliamente los conceptos abordados en los capítulos precedentes relacionados con la eficiencia del ancho de banda y los esquemas de codificación.

BERG96 Bergmans, J. *Digital Baseband Transmission and Recording*. Boston: Kluwer, 1996.

COUC01 Couch, L. *Digital and Analog Communication Systems*. Upper Saddle River, NJ: Prentice Hall, 2001.

FREE98 Freeman, R. «Bits, Symbols, Baud, and Bandwidth». *IEEE Communications Magazine*, abril 1998.

PEAR92 Pearson, J. *Basic Communication Theory*. Upper Saddle River, NJ: Prentice Hall, 1992.

PROA02 Proakis, J. *Communication Systems Engineering*. Upper Saddle River, NJ: Prentice Hall, 2002.

SKLA01 Sklar, B. *Digital Communications*: *Fundamentals and Applications*. Upper Saddle River, NJ: Prentice Hall, 2001.

SKLA93 Sklar, B. «Defining, Designing, and Evaluating Digital Communication Systems». *IEEE Communications Magazine*, noviembre 1993.

XION00 Xiong, F. *Digital Modulation Techniques*. Boston: Artech House, 2000.

5.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

aleatorización (*scrambling*)
AMI (*Alternate Mark Inversion*)
B8ZS (*Bipolar with* 8*-Zeros Substitution*)
bifase
binario multinivel
bipolar-AMI
codificación diferencial
eficiencia del ancho de banda
frecuencia portadora
HDB3 (*High-Density Bipolar*-3 *zeros*)
Manchester
Manchester diferencial
modulación
modulación angular
modulación de amplitud en cuadratura (QAM, *Quadrature Amplitude Modulation*)
modulación delta (DM, *Delta Modulation*)
modulación de amplitud (AM, *Amplitude Modulation*)
modulación de fase (PM, *Phase Modulation*)
modulación de frecuencia (FM, *Frequency Modulation*)
modulación por desplazamiento de amplitud (ASK, *Amplitude Shift Keying*)
modulación por desplazamiento de fase (PSK, *Phase Shift Keying*)
modulación por desplazamiento de frecuencia (FSK, *Frequency Shift Keying*)
modulación por impulsos codificados (PCM, *Pulse Code Modulation*)
modulación por impulsos de amplitud (PAM, *Pulse Amplitude Modulation*)
no retorno a cero (NRZ, *Non-Return to Zero*)
no retorno a nivel cero (NRZ-L, *Non-Return to Zero-Level*)
no retorno a cero invertido (NRZI, *Non-Return to Zero Inverted*)
polar
pseudoternario
PSK diferencial (DPSK, *Differential PSK*)
PSK en cuadratura (QPSK, *Quadrature PSK*)
señal en banda base
tasa de bits erróneos (BER, *Bit Error Rate*)
unipolar
velocidad de modulación

CUESTIONES DE REPASO

5.1. Enumere y defina brevemente los factores importantes que se deben usar para comparar y evaluar las distintas técnicas de codificación digital a digital.

5.2. ¿Qué es la codificación diferencial?

5.3. Explique las diferencias entre NRZ-L y NRZI.

5.4. Describa dos técnicas binarias multinivel de codificación digital a digital.

5.5. Defina la codificación bifase y describa dos técnicas de codificación bifase.

5.6. Explique la técnica de aleatorización en el contexto de la codificación digital a digital.

5.7. ¿Qué hace un módem?

5.8. ¿Cómo se representan los datos binarios usando modulación por desplazamiento de amplitud? ¿Qué limitaciones tiene esta aproximación?

5.9. ¿Cuál es la diferencia entre QPSK y QPSK desplazada?

5.10. ¿Qué es QAM?

5.11. ¿Qué enuncia el teorema de muestreo respecto a la frecuencia de muestreo necesaria para una señal analógica?

5.12. ¿Cuáles son las diferencias entre las modulaciones angulares PM y FM?

EJERCICIOS

5.1. ¿Cuál de las señales de la Tabla 5.2 usa codificación diferencial?

5.2. Obtengar los algoritmos que implementen cada uno de los códigos de la Tabla 5.2 a partir de NRZ-L.

5.3. A veces para las grabaciones en cintas magnéticas de alta densidad se usa una versión modificada del código NRZ, denominada NRZ-mejorado (E-NRZ, *Enhanced NRZ*). El E-NRZ implica la separación de la cadena de datos NRZ-L en palabras de 7 bits; se invierten los bits 2, 3, 6 y 7, y se añade un bit de paridad a cada palabra. El bit de paridad se elige para que el número total de unos en la palabra de 8 bits sea impar. ¿Qué ventajas tiene E-NRZ respecto NRZ-L? ¿Tiene desventajas?

5.4. Desarrolle el diagrama de estados (máquina de estados finitos) de la codificación pseudoternaria.

5.5. Considérese el siguiente esquema de codificación. A la entrada se tienen datos binarios, a_m, con $m = 1, 2, 3, \ldots$ Supóngase que se realiza un procesamiento en dos niveles. En primer lugar, se genera un conjunto de números binarios de acuerdo con la siguiente expresión

$$b_0 = 0$$
$$b_m = (a_m + b_{m-1}) \bmod 2$$

que se codifican de acuerdo con

$$c_m = b_m - b_{m-1}$$

En el receptor, los datos originales se recuperan mediante

$$a_m = c_m \bmod 2$$

a) Compruebe que los valores recibidos de a_m son iguales a los valores transmitidos.

b) ¿Qué tipo de codificación es ésta?

5.6. Para la cadena de bits 01001110, represente las formas de onda de cada uno de los códigos mostrados en la Tabla 5.2. Supóngase que en NRZI el nivel de la señal para codificar el bit anterior fue alto; que el bit 1 precedente en el esquema AMI correspondió a un nivel de tensión negativa; y que para el código pseudoternario el bit 0 más reciente se codificó con una tensión negativa.

5.7. La forma de onda de la Figura 5.25 corresponde a una cadena de bits codificada con código Manchester. Determine el principio y el final de los bits (es decir, extraiga la señal de reloj) y obtenga la secuencia de datos.

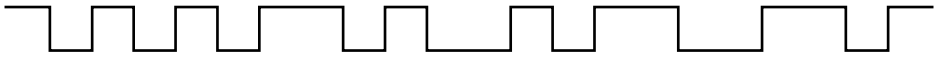


Figura 5.25. Secuencia Manchester.

5.8. Supóngase una secuencia de datos binarios formada por una serie larga de 1 consecutivos, seguida de un cero al que le sigue otra serie larga de 1; si se suponen las mismas condiciones que en el Ejercicio 5.6, dibuje la forma de onda correspondiente a esta secuencia si se codifica con

a) NRZ-L

b) Bipolar-AMI

c) Pseudoternario

5.9. Suponga que la forma de onda de un código bipolar-AMI correspondiente a la secuencia 0100101011 se transmite por un canal ruidoso. La forma de onda recibida se muestra en la Figura 5.26, en la que se ha incluido un error en un bit. Localice dónde está el error y justifique la respuesta.

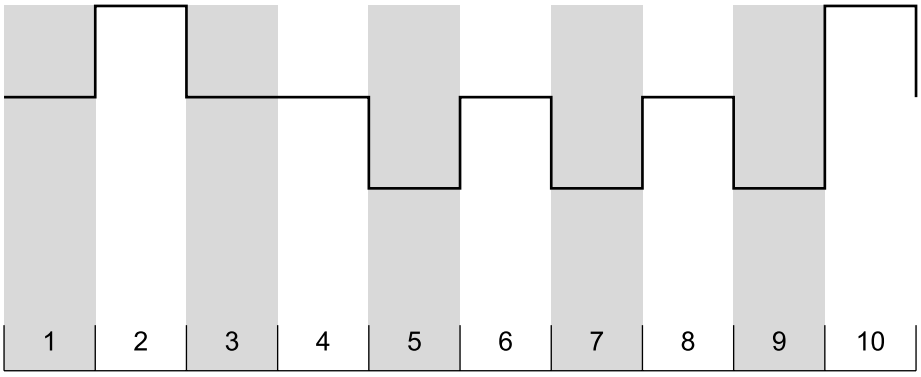


Figura 5.26. Forma de onda bipolar AMI recibida.

5.10. Una ventaja de la codificación bipolar es que una violación en la polaridad (es decir, dos pulsos + consecutivos, o dos pulsos − consecutivos, separados por un número indeterminado de ceros) le indicará al receptor que ha habido un error en la transmisión. Desafortunadamente, al recibir la violación, el receptor no puede determinar qué bit es erróneo (solamente detectará que ha ocurrido un error). Para la secuencia bipolar

$$+ - 0 + - 0 - +$$

la cual tiene una violación bipolar, determine dos secuencias de bits distintas que al ser transmitidas (con un bit erróneo) resulten en la misma secuencia anterior.

5.11. En la Figura 5.27 se muestra el demodulador QAM correspondiente al modulador QAM de la Figura 5.14. Muestre que este sistema recupera las dos señales $d_1(t)$ y $d_2(t)$, las cuales, si se combinaran darían lugar a la señal de entrada.

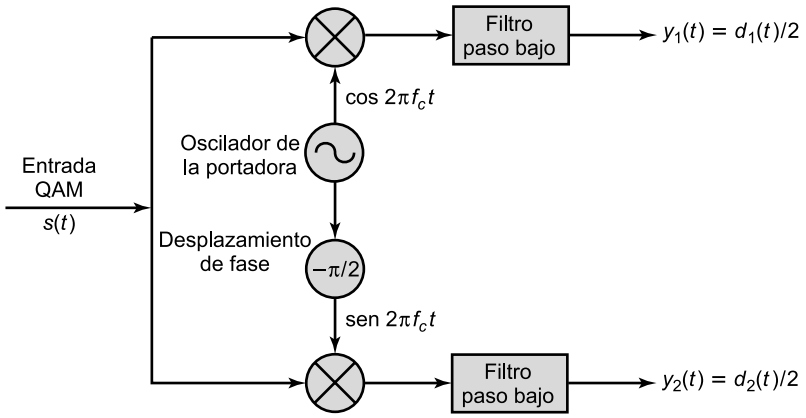


Figura 5.27. Demodulador QAM.

5.12. En los dos esquemas de señalización PSK y QPSK, se utiliza una onda seno. La duración del elemento de señalización es 10^{-5} segundos. Si la señal recibida es

$$s(t) = 0{,}005 \,\text{sen}\,(2\pi\, 10^6 t + \theta) \text{ voltios}$$

y el ruido en el receptor es $2{,}5 \times 10^{-8}$ vatios, determine E_b/N_0 (en dB) para cada caso.

5.13. Obténgase la expresión de la velocidad de modulación D (en baudios) en función de la velocidad de transmisión R para una modulación QPSK en la que se utilicen las técnicas de codificación digital mostradas en la Tabla 5.2.

5.14. ¿Qué SNR se necesita para conseguir una eficiencia del ancho de banda igual a 1,0 en los esquemas ASK, FSK, PSK y QPSK? Suponga que la tasa de errores por bit es 10^{-6}.

5.15. Una señal NRZ-L se pasa a través de un filtro con $r = 0{,}5$ y, posteriormente, se modula sobre una portadora. La velocidad de transmisión es 2.400 bps. Calcule el ancho de banda para ASK y FSK. Para FSK suponga que las frecuencias utilizadas son 50 kHz y 55 kHz.

5.16. Suponga que el canal de una línea telefónica se ecualiza para permitir la transmisión de datos en el rango de frecuencias de 600 hasta 3.000 Hz. El ancho de banda disponible es de 2.400 Hz. Para $r = 1$, calcule el ancho de banda necesario para QPSK a 2.400 bps y para

4.800 bps, ambas con ocho bits de señalización multinivel. ¿Es dicho ancho de banda adecuado?

5.17. En la codificación de señales analógicas que representen datos digitales, ¿por qué PCM es preferible a DM?

5.18. ¿Es el módem un dispositivo que realiza las funciones inversas de un *codec*? Es decir, ¿podría un módem funcionar como un *codec* invertido o viceversa?

5.19. Una señal se cuantiza utilizando 10 bits PCM. Calcule la relación señal-ruido de cuantización.

5.20. Considere una señal de audio cuyas componentes espectrales estén comprendidas en el rango de 300 a 3.000 Hz. Suponga que se usa una frecuencia de muestreo de 7.000 muestras por segundo para generar una señal PCM.

a) Para una SNR = 30 dB, ¿cuántos niveles se necesitan en un cuantizador uniforme?

b) ¿Cuál es la velocidad de transmisión necesaria?

5.21. Determine el tamaño del escalón δ que se necesita para evitar el ruido de sobrecarga en la pendiente en función de la componente máxima en frecuencias de la señal. Suponga que todas las componentes tienen amplitud A.

5.22. Un codificador PCM acepta señales en un rango de 10 voltios de tensión y genera códigos de 8 bits usando cuantización uniforme. La tensión máxima normalizada cuantizada es $1 - 2^{-8}$. Determine:

a) El tamaño del escalón normalizado.

b) El tamaño del escalón real en voltios.

c) El máximo nivel cuantizado en voltios.

d) La resolución normalizada.

e) La resolución real.

f) El porcentaje de resolución.

5.23. La forma de onda analógica que se muestra en la Figura 5.28 se va a codificar usando modulación delta. El periodo de muestreo y el tamaño del escalón se muestran en la figura mediante una cuadrícula. En la misma figura se muestran la primera salida DM y la correspondiente función escalera. Obtener el resto de la función escalera y la salida DM. Indique las regiones en las que haya distorsión de sobrecarga en la pendiente.

5.24. Para la señal modulada en ángulo correspondiente a la siguiente expresión

$$s(t) = 10\cos[(10^8)\pi t + 5\,\text{sen}\,2\pi(10^3)t]$$

determine la máxima desviación de fase y la máxima desviación en frecuencia.

5.25. Supóngase la señal modulada en ángulo correspondiente a la siguiente expresión

$$s(t) = 10\cos[2\pi(10^6)t + 0{,}1\,\text{sen}\,(10^3)\pi t]$$

a) Exprese $s(t)$ como una señal PM, siendo $n_p = 10$.

b) Exprese $s(t)$ como una señal FM, siendo $n_f = 10$p.

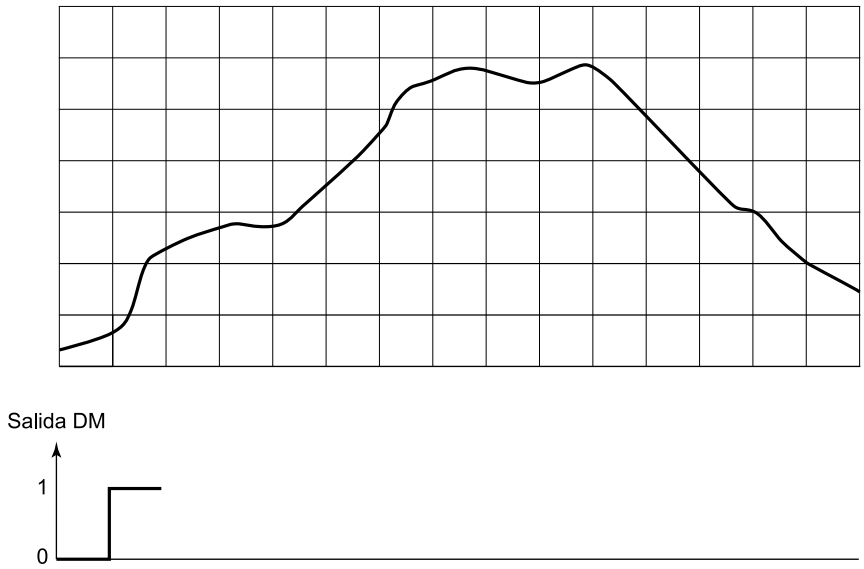


Figura 5.28. Ejemplo de modulación delta.

5.26. Sean $m_1(t)$ y $m_2(t)$ dos señales correspondientes a dos mensajes. Sean $s_1(t)$ y $s_2(t)$ las correspondientes señales moduladas, en las que se ha utilizado una portadora de frecuencia f_c.

a) Demuestre que, si se utiliza un sencillo esquema AM, $m_1(t) + m_2(t)$ genera una señal modulada igual a una combinación lineal de $s_1(t)$ y $s_2(t)$. Esto justifica el por qué, a veces, a AM se le denomina modulación lineal.

b) Demuestre que, si se utiliza un esquema simple PM, entonces $m_1(t) + m_2(t)$ genera una señal modulada no igual a una combinación lineal de $s_1(t)$ y $s_2(t)$. Esto justifica el por qué, a veces, a PM se le denomina modulación no lineal.

CAPÍTULO 6

Técnicas de comunicación de datos digitales

6.1. Transmisión asíncrona y síncrona
Transmisión asíncrona
Transmisión síncrona

6.2. Tipos de errores

6.3. Detección de errores
Comprobación de paridad
Comprobación de redundancia cíclica (CRC)

6.4. Corrección de errores
Principios generales de los códigos de bloque

6.5. Configuraciones de línea
Topología
Full-duplex y *half-duplex*

6.6. Interfaces
V.24/EIA-232-F
Interfaz física de RDSI

6.7. Lecturas recomendadas

6.8. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- La transmisión de una cadena de bits desde un dispositivo a otro, a través de una línea de transmisión, implica un alto grado de cooperación entre ambos extremos. Uno de los requisitos esenciales es la **sincronización.** El receptor debe saber la velocidad a la que se están recibiendo los datos, de tal manera que pueda muestrear la línea a intervalos constantes de tiempo para así determinar cada uno de los bits recibidos. Para este propósito, se utilizan habitualmente dos técnicas. En la **transmisión asíncrona,** cada carácter se trata independientemente. El primer bit de cada carácter es un bit de comienzo que alerta al receptor sobre la llegada del carácter. El receptor muestrea cada bit del carácter y busca el comienzo del siguiente. Esta técnica puede que no funcione correctamente para bloques de datos excesivamente largos debido a que el reloj del receptor podría perder el sincronismo respecto del emisor. No obstante, la transmisión de datos en bloques grandes es más eficaz que la transmisión carácter a carácter. Para el envío de bloques grandes se utiliza **la transmisión síncrona.** Cada bloque de datos forma una trama la cual incluirá, entre otros campos, los delimitadores de principio y de fin. Al transmitir la trama se empleará alguna técnica de sincronización, por ejemplo, la obtenida con el código Manchester.
- La **detección de errores** se lleva a cabo calculando un código en función de los bits de entrada. El código se añade a los bits a transmitir. Para comprobar si ha habido errores, el receptor calcula el código en función de los bits recibidos y lo compara con el código recibido.
- La **corrección de errores** opera de forma similar a la detección de errores, pero en este caso será posible corregir ciertos errores en la secuencia de bits recibida.
- Para transmitir a través de un medio, todo dispositivo lo hará mediante alguna **interfaz.** La interfaz no sólo define las características eléctricas de la señal sino que, además, especifica la conexión física, así como los procedimientos para enviar y recibir bits.

En los tres capítulos anteriores se han estudiado fundamentalmente los aspectos principales de la transmisión de datos, como la caracterización de las señales y los medios de transmisión, la codificación de señales y la medida de las prestaciones. En este capítulo centraremos nuestra atención en la comunicación de datos.

Para que dos dispositivos conectados por un medio de transmisión intercambien datos es necesario un alto grado de cooperación. Normalmente, los datos se transmiten bit a bit a través del medio; la temporización (es decir, la velocidad de transmisión, la duración y la separación entre bits) de estos bits debe ser común en el receptor y en el transmisor. En la Sección 6.1 se estudian dos técnicas que son habituales para el control de la temporización: la transmisión síncrona y la asíncrona. En la sección siguiente se estudia el problema de los errores. Como ya se ha comentado, la transmisión de datos no es un proceso libre de errores, por lo que será necesario algún mecanismo que los controle. Tras un breve estudio, en el que se distingue entre errores en bits aislados y errores a ráfagas, en este capítulo se presentan dos enfoques para tratar los errores: la detección de errores y la corrección de errores.

A continuación se revisan las configuraciones más habituales en las líneas de transmisión. Finalmente, se estudia la interfaz física entre los dispositivos de transmisión de datos y la línea de transmisión. Normalmente, los dispositivos de datos digitales no se conectan directamente a través del medio. En su lugar, la conexión se realiza a través de una interfaz normalizada que proporciona un control considerable sobre la interacción de los dispositivos de recepción/emisión con la línea de transmisión.

6.1. TRANSMISIÓN ASÍNCRONA Y SÍNCRONA

En este texto se estudia fundamentalmente la transmisión serie de datos, es decir, la transmisión de datos a través de un único camino, en lugar de utilizar un conjunto de líneas en paralelo, como es habitual en los dispositivos de E/S y en los buses internos de los computadores. En la transmisión serie, los elementos de señalización se envían a través de la línea de transmisión de uno en uno. Cada elemento puede ser:

- **Menor que un bit:** como en el caso de la codificación Manchester.
- **Un bit:** NRZ-L es un ejemplo digital y FSK es un ejemplo analógico.
- **Mayor que un bit:** como por ejemplo en QPSK.

Para simplificar, en el razonamiento que sigue, mientras no se especifique lo contrario, supondremos que se usa un bit por elemento de señalización. Esta simplificación no va a influir en el tratamiento llevado a cabo.

Recuérdese que (*véase* Figura 3.15) para determinar el valor binario en la recepción de los datos digitales se realiza un muestreo de la señal por cada bit recibido. En este caso, los defectos en la transmisión pueden corromper la señal de tal manera que se cometan errores ocasionales. El problema anterior se agrava por la dificultad adicional de la temporización: para que el receptor muestree los bits recibidos correctamente debe conocer el instante de llegada, así como la duración de cada bit.

Supóngase que el emisor emite una cadena de bits. Esto se hará de acuerdo con el reloj del transmisor. Por ejemplo, si los datos se transmiten a un millón de bits por segundo (1 Mbps), significará que se transmite un bit cada $1/10^6 = 1$ microsegundo (μs), medidos con el reloj del emisor. Generalmente, el receptor intentará muestrear el medio en la parte central de cada bit, obteniendo una muestra por cada intervalo de duración de un bit. En el ejemplo, el muestreo se hará cada 1 μs. Si el receptor delimita las duraciones basándose en su propio reloj, se puede presentar un problema si los dos relojes (el del emisor y el del receptor) no están sincronizados con precisión. Si hay una pérdida de sincronismo del 1 por ciento (el reloj del receptor es un 1 por ciento más rápido, o lento, que el reloj del transmisor), entonces el primer muestreo estará desplazado 0,01 veces la duración del bit (0,01 μs) del instante central del intervalo (es decir, a 0,5 μs del principio o del final del intervalo). Tras 50 muestras, o más, el receptor puede obtener un error debido a que el muestreo lo realizará en un instante incorrecto ($50 \times 0{,}01 = 0{,}5$ μs). Si la pérdida de sincronismo fuera menor, el error ocurriría más tarde. En cualquier caso, si se emite un número suficiente de bits, dicho error aparecerá irremediablemente si no se adoptan medidas para sincronizar al transmisor y al receptor.

TRANSMISIÓN ASÍNCRONA

Hay dos enfoques habituales para resolver el problema de la sincronización. El primero se denomina, de una manera no muy acertada, transmisión asíncrona. En esta aproximación, el problema de la temporización se evita no enviando cadenas de bits largas de forma ininterrumpida. En su lugar, los datos se transmiten enviándolos carácter a carácter. Normalmente, cada carácter tiene una longitud de 5 a 8 bits[1]. La temporización o sincronización se debe mantener solamente durante

[1] El número de bits correspondiente a cada carácter depende del código que se utilice. Ya se ha mencionado un ejemplo, el código IRA, en el que se usan siete bits por carácter. Otro código habitual es el EBCDIC (*Extended Binary Coded Decimal Interchange Code*), que es de 8 bits y se utiliza en todas las máquinas de IBM, excepto en los computadores personales y estaciones de trabajo.

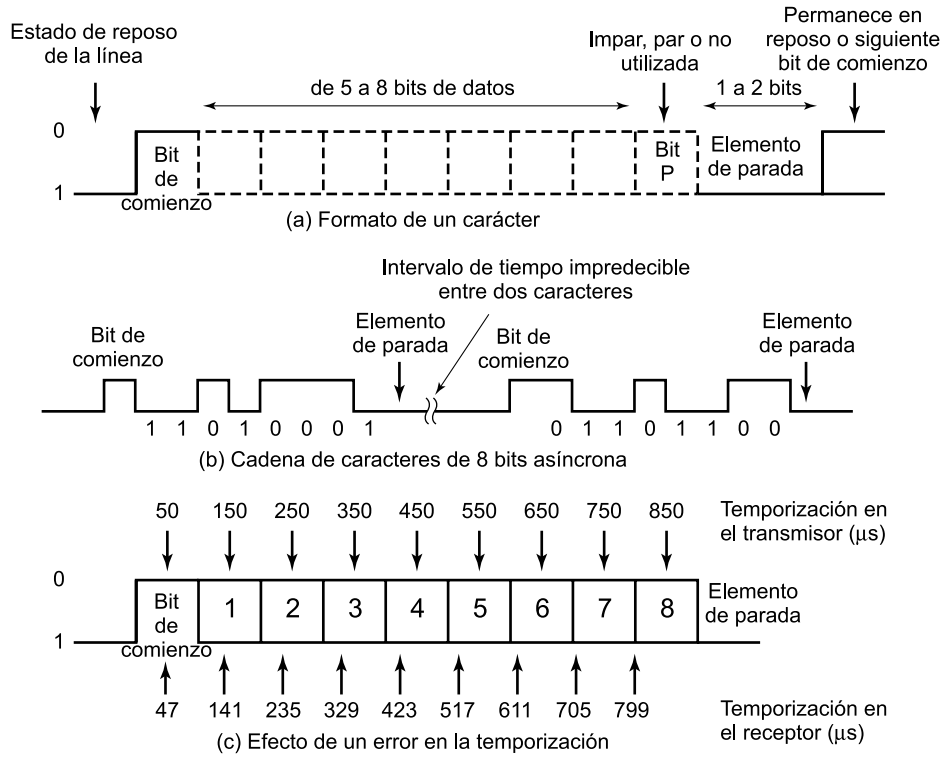

Estado de reposo de la línea
Impar, par o no utilizada
Permanece en reposo o siguiente bit de comienzo
de 5 a 8 bits de datos
1 a 2 bits
0
1
Bit de comienzo
Bit P
Elemento de parada
(a) Formato de un carácter
Intervalo de tiempo impredecible entre dos caracteres
Bit de comienzo
Elemento de parada
Bit de comienzo
Elemento de parada
1 1 0 1 0 0 0 1
0 1 1 0 1 1 0 0
(b) Cadena de caracteres de 8 bits asíncrona
50 150 250 350 450 550 650 750 850
Temporización en el transmisor (μs)
0
1
Bit de comienzo
1 2 3 4 5 6 7 8
Elemento de parada
47 141 235 329 423 517 611 705 799
Temporización en el receptor (μs)
(c) Efecto de un error en la temporización

Figura 6.1. Transmisión asíncrona.

la duración del carácter, ya que el receptor tiene la oportunidad de resincronizarse al principio de cada nuevo carácter.

Esta técnica se va a explicar con la ayuda de la Figura 6.1. Cuando no se transmite ningún carácter, la línea entre el emisor y el receptor estará en estado de *reposo*. La definición de *reposo* es equivalente al elemento de señalización correspondiente al 1 binario. Así, en la señalización NRZ-L (*véase* Figura 5.2), habitual en la transmisión asíncrona, el estado de reposo correspondería con la presencia de una tensión negativa en la línea. El principio de cada carácter se indica mediante un *bit de comienzo* que corresponde al valor binario 0. A continuación se transmite el carácter, comenzando por el bit menos significativo, que tendrá entre cinco y ocho bits. A modo de ejemplo, en los caracteres IRA, a los bits de datos se les añade un bit de paridad, el cual ocupa, por tanto, la posición correspondiente al bit más significativo. El bit de paridad se determina en el emisor, de tal manera que el número de unos dentro del carácter, incluyendo el bit de paridad, sea par (paridad par) o impar (paridad impar), dependiendo del criterio que se elija. Este bit se usa en el receptor para la detección de errores, como se explica en la Sección 6.3. Por último, está el denominado *elemento de parada*, que corresponde a un 1 binario. Se debe especificar la longitud mínima del elemento de parada, la cual normalmente es igual a 1, 1,5 o 2 veces la duración de un bit convencional. No se especifica un valor máximo. Debido a que el elemento de parada es igual que el estado de reposo, el transmisor seguirá transmitiendo la señal de parada hasta que se transmita el siguiente carácter.

Este esquema no es muy exigente en cuanto a los requisitos de temporización. Por ejemplo, usualmente los caracteres IRA se envían como unidades de 8 bits, incluyendo el bit de paridad. Si

el receptor es un 5 por ciento más rápido, o más lento, que el emisor, el octavo muestreo estará desplazado un 45 por ciento, lo que significa que todavía es aceptable. En la Figura 6.1c se muestra el efecto de un error de temporización lo suficientemente grande como para provocar un error en la recepción. En este ejemplo supondremos una velocidad de transmisión de 10.000 bits por segundo (10 kbps); por tanto, se transmite un bit cada 0,1 milisegundos (ms), es decir, tiene una duración de 100 μs. Supongamos que el receptor está fuera de sincronismo un 6 por ciento, es decir, en 6 μs cada intervalo de duración de un bit. Por tanto, el receptor muestrea el carácter de entrada cada 94 μs (medidos con el reloj del transmisor). Como se puede observar, la última muestra será errónea.

Un error como el anterior en realidad dará lugar a dos errores. Primero, el último bit muestreado será incorrecto, y segundo, la cuenta de bits puede estar desalineada. Si el bit 7 es un 1 y el bit 8 es un 0, el bit 8 se puede interpretar erróneamente como un bit de comienzo. Este tipo de error se denomina *error de delimitación de trama*, ya que a la unidad constituida por el carácter más el bit de comienzo y el elemento de parada se denomina trama. Se puede dar igualmente un error de delimitación de trama si el ruido hace que se detecte un bit de comienzo erróneamente durante el estado de reposo.

La transmisión asíncrona es sencilla y de bajo coste, si bien requiere 2 o 3 bits suplementarios por cada carácter. Por ejemplo, en un código de 8 bits sin bit de paridad y con un elemento de parada de duración 1 bit, de cada diez bits, dos no contendrán información ya que se dedicarán a la sincronización; por tanto, los bits suplementarios llegan a un 20 por ciento. Por descontado que el porcentaje de bits suplementarios se podría reducir mediante la transmisión de bloques con más bits entre el bit de comienzo y el de parada. No obstante, como se muestra en la Figura 6.1c, cuanto mayor sea el bloque de bits, mayor será el error de temporización acumulativo. Para conseguir un mejor rendimiento en la sincronización se puede usar una estrategia diferente denominada transmisión síncrona.

TRANSMISIÓN SÍNCRONA

En la transmisión síncrona, cada bloque de bits se transmite como una cadena estacionaria sin utilizar códigos de comienzo o parada. El bloque puede tener una longitud de muchos bits. Para prevenir la pérdida de sincronismo entre el emisor y el receptor, sus relojes se deberán sincronizar de alguna manera. Una posibilidad puede ser proporcionar la señal de reloj a través de una línea independiente. Uno de los extremos (el receptor o el transmisor) enviará regularmente un pulso de corta duración. El otro extremo utilizará esta señal a modo de reloj. Esta técnica funciona bien a distancias cortas. Sin embargo, a distancias superiores, los pulsos de reloj pueden sufrir las mismas dificultades y defectos que las propias señales de datos, por lo que pueden aparecer errores de sincronización. La otra alternativa consiste en incluir la información relativa a la sincronización en la propia señal de datos. En señalización digital, esto se puede llevar a cabo mediante la codificación Manchester o Manchester diferencial. En señalización analógica se han desarrollado, a su vez, varias técnicas; por ejemplo, usando la fase de la propia portadora.

En la transmisión síncrona se requiere además un nivel de sincronización adicional para que el receptor pueda determinar dónde está el comienzo y el final de cada bloque de datos. Para llevar a cabo esto, cada bloque comienza con un patrón de bits denominado *preámbulo* y, por lo general, termina con un patrón de bits denominado *final*. Además de los anteriores, se añaden otros bits que se utilizan en los procedimientos de control del enlace estudiados en el Capítulo 7. Al conjunto de bits, o unidad de información formada por los datos más el preámbulo más los bits de final junto con la información de control se le denomina **trama**. El formato en particular de la trama dependerá del procedimiento de control del enlace que se utilice.

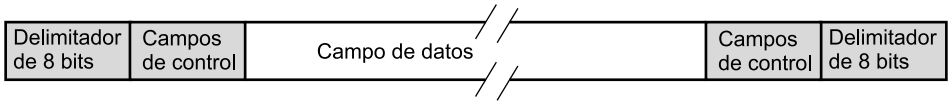


Figura 6.2. Formato de una trama síncrona.

En la Figura 6.2 se muestra, en términos generales, un formato típico de una trama en una transmisión síncrona. Normalmente, la trama comienza con un preámbulo de 8 bits llamado delimitador (*flag*). El mismo delimitador se utiliza igualmente como indicador del final de la trama. El receptor buscará la aparición del delimitador que determina el comienzo de la trama. Este delimitador estará seguido por algunos campos de control, el campo de datos (de longitud variable para la mayoría de los protocolos), más campos de control y, por último, se repetirá el delimitador indicando el final de la trama.

Para los bloques de datos que sean suficientemente grandes, la transmisión síncrona es mucho más eficiente que la asíncrona. La transmisión asíncrona requiere un 20 por ciento, o más, de bits suplementarios. La información de control, el preámbulo y el final son normalmente menos de 100 bits. Por ejemplo, en HDLC, uno de los esquemas más utilizados (estudiado en el Capítulo 7), se definen 48 bits de control, preámbulo y final. Por tanto, por cada bloque de datos de 1.000 caracteres, cada trama contendrá 48 bits de bits suplementarios y $1.000 \times 8 = 8.000$ bits de datos, lo que corresponde a un porcentaje de bits suplementarios igual a $48/8.048 \times 100\% = 0{,}6\%$ solamente.

6.2. TIPOS DE ERRORES

En los sistemas de transmisión digital, se dice que ha habido un error cuando se altera un bit. Es decir, cuando se transmite un 1 binario y se recibe un 0, o cuando se transmite un 0 binario y se recibe un 1. Existen dos tipos de errores: errores aislados o errores a ráfagas. Los primeros corresponden con eventualidades que alteran a un solo bit, sin llegar a afectar a los vecinos. Por el contrario, se dice que ha habido una ráfaga de longitud B cuando se recibe una secuencia de B bits en la que el primero, el último y cualquier número de bits intermedios son erróneos. De forma más precisa, la norma IEEE 100 define una ráfaga de errores como:

> **Ráfaga de errores:** grupo de bits en el que dos bits erróneos cualquiera estarán siempre separados por menos de un número x de bits correctos. El último bit erróneo en l ráfaga y el primer bit erróneo de la siguiente estarán, consecuentemente, separados por al menos x bits correctos.

Por tanto, en una ráfaga de errores habrá un conjunto de bits con un número dado de errores, aunque no necesariamente todos los bits en el conjunto sean erróneos.

Un error aislado se puede dar en presencia de ruido blanco, cuando cualquier deterioro aleatorio en la relación señal-ruido sea suficiente para confundir al receptor en un único bit. Por lo general, las ráfagas son más frecuentes y más difíciles de tratar. Pueden estar causadas por ruido impulsivo, descrito en el Capítulo 3. En entornos de comunicación móvil, otra causa para las ráfagas son los desvanecimientos, descritos en el Capítulo 14.

Téngase en cuen ta que los efectos de una ráfaga serán siempre mayores cuanto mayor sea la velocidad de transmisión.

Ejemplo 6.1. Supóngase un ruido impulsivo o un desvanecimiento de 1 μs. A una velocidad de transmisión de 1 Mbps causará una ráfaga de 10 bits. A 100 Mbps la ráfaga será de 100 bits.

6.3. DETECCIÓN DE ERRORES

En todo sistema de transmisión habrá ruido, independientemente de cómo haya sido diseñado. El ruido dará lugar a errores que modificarán uno o varios bits de la trama. En lo que sigue, se supondrá que los datos se transmiten mediante una o varias secuencias contiguas de bits, denominadas tramas.

A continuación, se definen las siguientes probabilidades para los posibles errores en las tramas transmitidas:

P_b: Probabilidad de que un bit recibido sea erróneo, también se denomina tasa de error por bit (BER, *Bit Error Rate*).

P_1: probabilidad de que una trama llegue sin errores.

P_2: probabilidad de que, utilizando un algoritmo para la detección de errores, una trama llegue con uno o más errores no detectados.

P_3: probabilidad de que, utilizando un algoritmo para la detección de errores, una trama llegue con uno o más errores detectados y sin errores indetectados.

En primer lugar, se considerará el caso en el que no se toman medidas para detectar errores. En ese caso, la probabilidad de errores detectados (P_3) es cero. Para calcular las otras probabilidades se supondrá que todos los bits tienen una probabilidad de error (P_b) constante e independiente. Entonces se tiene que:

$$P_1 = (1 - P_b)^F$$
$$P_2 = 1 - P_1$$

donde F es el número de bits por trama. Dicho en palabras, como cabría esperar, la probabilidad de que una trama llegue sin ningún bit erróneo disminuye al aumentar la probabilidad de que un bit sea erróneo. Además, la probabilidad de que una trama llegue sin errores disminuye al aumentar la longitud de la misma; cuanto mayor es la trama, mayor número de bits tendrá, y mayor será la probabilidad de que alguno de los bits sea erróneo.

Ejemplo 6.2. Un objetivo predefinido en las conexiones RDSI es que la BER en un canal a 64 kbps debe ser menor que 10^{-6} para, por lo menos, el 90% de los intervalos observados de 1 minuto de duración. Supóngase ahora que se tiene un usuario con requisitos menos exigentes para el que, en el mejor de los casos, una trama con un bit erróneo no detectable ocurriera por cada día de funcionamiento continuo en una canal a 64 kbps. Supóngase que la longitud de la trama es de 1.000 bits. El número de tramas que se pueden transmitir por día es $5{,}529 \times 10^6$, lo que implica una tasa de tramas erróneas $P_2 = 1/(5{,}529 \times 10^6) = 0{,}18 \times 10^{-6}$. Pero si se supone un valor de P_b igual a 10^{-6}, entonces $P_1 = (0{,}999999)^{1000} = 0{,}999$ y, por tanto, $P_2 = 10^{-3}$, lo que está tres órdenes de magnitud por encima de lo requerido.

Éste es el tipo de resultados que justifica el uso de técnicas para la detección de errores. Todas ellas se basan en el siguiente principio (*véase* Figura 6.3). Dada una trama de bits, se añaden bits

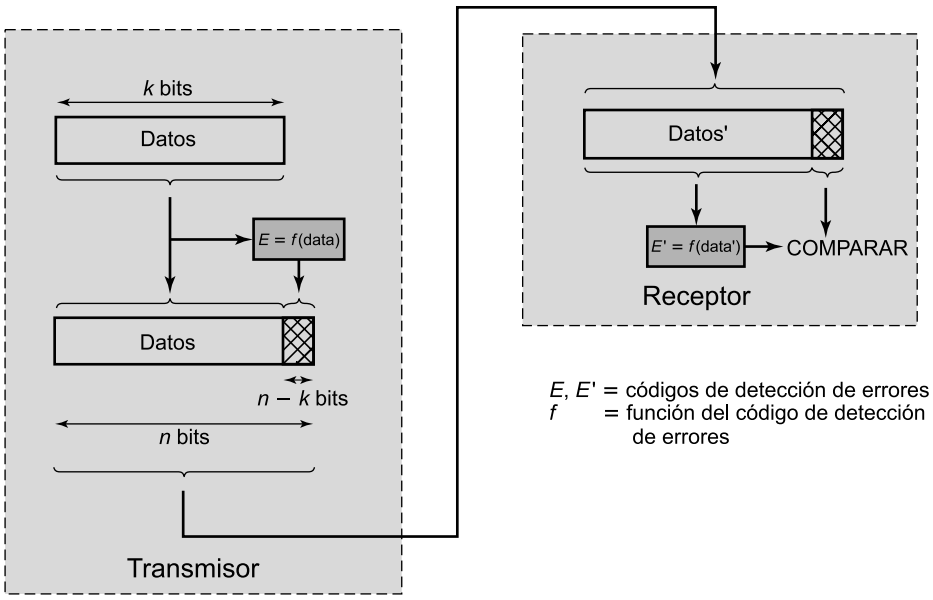


Figura 6.3. Procedimiento para detectar errores.

adicionales por parte del transmisor para formar un código con capacidad de detectar errores. Este código se calculará en función de los otros bits que se vayan a transmitir. Generalmente, para un bloque de datos de k bits, el algoritmo de detección de errores utiliza un código de $n - k$ bits, siendo $(n - k) < k$. El código de detección de errores, también llamado **bits de comprobación,** se añade al bloque de datos para generar la trama de n bits de longitud, la cual será posteriormente transmitida. El receptor separará la trama recibida en los k bits de datos y los $(n - k)$ bits correspondientes al código de detección de errores. El receptor realizará el mismo cálculo sobre los bits de datos recibidos y comparará el resultado con los bits recibidos en el código de detección de errores. Se detectará un error si, y solamente si, los dos resultados mencionados no coinciden. Por tanto, P_3 es la probabilidad de que la trama contenga errores y el sistema los detecte. P_2 se denomina tasa de error residual y se define como la probabilidad de que no se detecte un error aunque se esté usando un esquema de detección de errores.

COMPROBACIÓN DE PARIDAD

El esquema más sencillo para detectar errores consiste en añadir un bit de paridad al final de cada bloque de datos. Un ejemplo típico es la transmisión de caracteres en la que se añade un bit de paridad por cada carácter IRA de 7 bits. El valor de este bit se determina de tal forma que el carácter resultante tenga un número impar de unos (paridad impar) o un número par (paridad par).

Ejemplo 6.3. Si el transmisor está transmitiendo una G en IRA (1110001) y utiliza paridad impar, añadirá un 1 y transmitirá 11110001[2]. El receptor examinará el carácter recibido y si el

[2] Recuérdese del Apartado 5.1 que el bit menos significativo de un carácter se transmite primero y que el bit de paridad es el bit más significativo.

número total de unos es impar, supondrá que no ha habido errores. Si un bit (o cualquier número impar de bits) se invierte erróneamente durante la transmisión (por ejemplo, 11000011), entonces el receptor detectará un error.

Nótese, no obstante, que si dos (o cualquier número par) de bits se invierten debido a un error, aparecerá un error no detectado. Normalmente, se utiliza paridad par para la transmisión síncrona y paridad impar para la asíncrona.

La utilización de bits de paridad no es infalible, ya que los impulsos de ruido son, a menudo, lo suficientemente largos como para destruir más de un bit, especialmente a velocidades de transmisión altas.

COMPROBACIÓN DE REDUNDANCIA CÍCLICA (CRC)

Uno de los códigos para la detección de errores más habitual y más potente son los de comprobación de redundancia cíclica (CRC, *Cyclic Redundancy Check*), que se pueden explicar de la siguiente manera. Dado un bloque o mensaje de k-bits, el transmisor genera una secuencia de $(n - k)$ bits, denominada secuencia de comprobación de la trama (FCS, *Frame Check Sequence*), de tal manera que la trama resultante, con n bits, sea divisible por algún número predeterminado. El receptor dividirá la trama recibida entre ese número y si no hay resto en la división, supondrá que no ha habido errores[3].

Para clarificar el funcionamiento de este procedimiento, a continuación se va a explicar de tres maneras: usando aritmética módulo 2, mediante polinomios y usando lógica digital.

Aritmética módulo 2

La aritmética módulo 2 hace uso de sumas binarias sin acarreo, lo cual es exactamente igual que la operación lógica *exclusive-OR*. La operación de resta binaria sin acarreos es también igual que la operación lógica *exclusive-OR*. Por ejemplo:

$$\begin{array}{r} 1111 \\ +\,1010 \\ \hline 0101 \end{array} \qquad \begin{array}{r} 1111 \\ -\,0101 \\ \hline 1010 \end{array} \qquad \begin{array}{r} 11001 \\ \times\ 11 \\ \hline 11001 \\ 11001 \\ \hline 101011 \end{array}$$

Algunas definiciones:

T = trama de n bits a transmitir.

M = mensaje con k bits de datos, correspondientes con los primeros k bits de T.

F = $(n - k)$ bits de FCS, los últimos $(n - k)$ bits de T.

P = patrón de $n - k + 1$ bits; éste es el divisor elegido.

El objetivo es que la división T/P no tenga resto alguno. Es evidente que

$$T = 2^{n-k}D + F$$

[3] Este procedimiento es ligeramente diferente al de la Figura 6.3. Como se verá más adelante, el procedimiento de la CRC se puede realizar de la siguiente manera. El receptor podría realizar una división sobre los bits de datos de entrada y comparar el resultado con los bits de comprobación.

Es decir, multiplicar D por 2^{n-k} en realidad equivale a desplazar hacia la izquierda $n - k$ bits, añadiendo ceros al resultado. Finalmente, en la obtención de T, al sumar F lo que estamos haciendo es, en realidad, concatenar D y F. El objetivo es hacer T divisible entre P. Supóngase que se divide $2^{n-k}D$ entre P:

$$\frac{2^{n-k}D}{P} = Q + \frac{R}{P} \tag{6.1}$$

Hay un cociente y un resto. El resto será siempre al menos un bit más corto que el divisor, ya que la división es módulo 2. La secuencia de comprobación de la trama, o FCS, será igual al resto de la división. Entonces

$$T = 2^{n-k}D + R \tag{6.2}$$

¿Satisface R la condición exigida de que la división T/P tenga resto cero? Para comprobarlo considérese que

$$\frac{T}{P} = \frac{2^{n-k}D + R}{P} = \frac{2^{n-k}D}{P} + \frac{R}{P}$$

Sustituyendo en la Ecuación (6.1)[4], se tiene que

$$\frac{T}{P} = Q + \frac{R}{P} + \frac{R}{P}$$

No obstante, cualquier número binario sumado a módulo 2 consigo mismo es igual a cero. Por tanto,

$$\frac{T}{P} = Q + \frac{R + R}{P} = Q$$

No hay resto y, por tanto, T es divisible entre P. Así pues, la FCS se genera fácilmente: simplemente se divide $2^{n-k}D$ entre P y se usan los $(n - k)$ bits del resto como FCS. En el receptor se dividirá T entre P y, si no ha habido errores, no se obtendrá resto alguno.

Ejemplo 6.4.

1. Sean:

mensaje D = 1010001101 (10 bits)

patrón P = 110101 (6 bits)

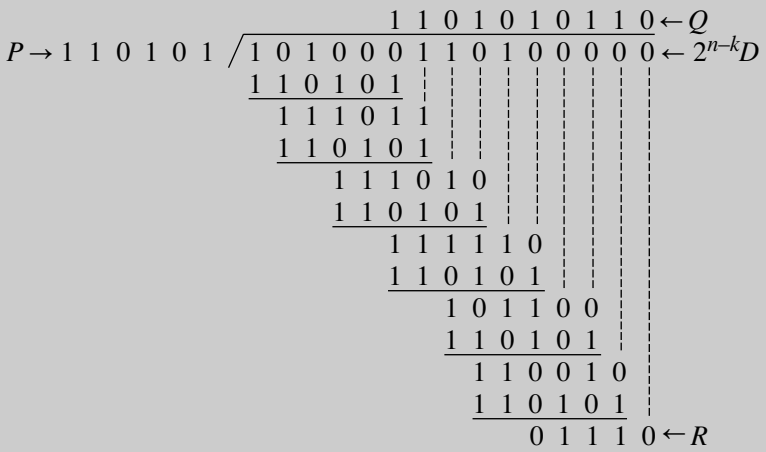
FCS R = a calcular (5 bits)

Por tanto, $n = 15$, $k = 10$ y $(n - k) = 5$.

2. El mensaje se multiplica por 2^5, resultando 101000110100000.

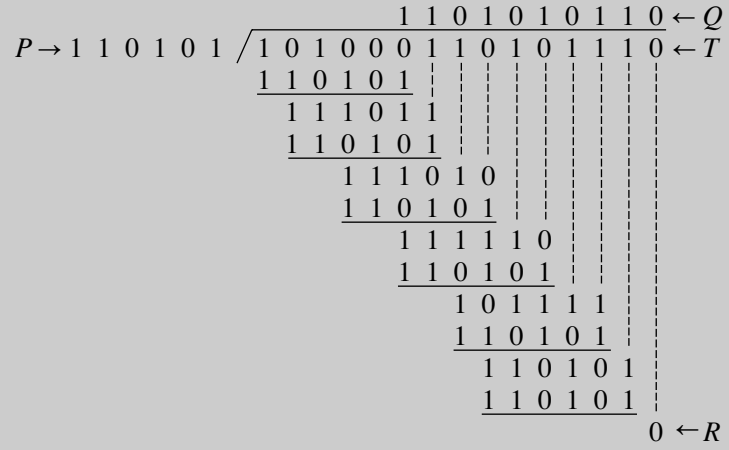
[4] *N. del T.:* Hay una errata en la edición inglesa.

3. El resultado anterior se divide entre P:



4. El resto se suma a $2^5\ D$ para dar $T = 101000110101110$, que es lo que se transmite.

5. Si no hay errores, el receptor recibe T intacto. La trama recibida se divide entre P:



Ya que no hay resto, se supone que no ha habido errores.

El patrón P se elige con un bit más que la longitud de la FCS deseada. El patrón elegido en particular, dependerá del tipo de errores que se espera sufrir. Como mínimo, el bit más significativo y el menos significativo de P deben ser 1.

Hay un método conciso para detectar la presencia de uno o más errores. Un error provocará que se invierta un bit. Esto es equivalente a calcular la función *exclusive-OR* entre el bit y 1 (es decir, sumar módulo 2 un 1 a dicho bit): $0 + 1 = 1$; $1 + 1 = 0$. Por tanto, los errores en una trama de n bits se pueden representar mediante una palabra de n bits, teniendo 1 en aquellas posiciones que coincidan con un error. La trama T_r resultante se puede expresar como

$$T_r = T \oplus E$$

donde

T = trama transmitida.

E = patrón de errores con 1 en las posiciones donde haya un error.

T_r = trama recibida.

Si ha habido un error ($E \neq 0$), el receptor fallará en la detección si, y solamente si, T_r es divisible entre P, lo que es equivalente a que E sea divisible entre P. Intuitivamente, esto parece que es un evento improbable.

Polinomios

Una segunda forma de ver el proceso de CRC es expresar todos los valores como polinomios de una variable muda X, con coeficientes binarios. Los coeficientes corresponderán con los bits del número en binario. Así, si $D = 110011$, se tendrá que $D(X) = X^5 + X^4 + X + 1$, y si $P = 11001$, se tiene que $P(X) = X^4 + X^3 + 1$. De nuevo, las operaciones se realizan en aritmética módulo 2. El procedimiento de CRC se puede describir de la siguiente manera:

$$\frac{X^{n-k}D(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$T(X) = X^{n-k}D(X) + R(X)$$

Compare estas Ecuaciones con (6.1) y (6.2).

Ejemplo 6.5. Utilizando el ejemplo anterior, para $D = 1010001101$, se tiene que $D(X) = X^9 + X^7 + X^3 + X^2 + 1$, y para $P = 110101$, se tiene que $P(X) = X^5 + X^4 + X^2 + 1$. Se obtendrá $R = 01110$, que corresponde con $R(X) = X^3 + X^2 + X$. La Figura 6.4 muestra la división polinómica que corresponde con la división binaria del ejemplo anterior.

Un error $E(X)$ no se detectará solamente si es divisible entre $P(X)$. Se puede demostrar [PETE61, RAMA88] que los siguientes errores no son divisibles y, por tanto, se podrán detectar, si se elige adecuadamente el polinomio $P(X)$:

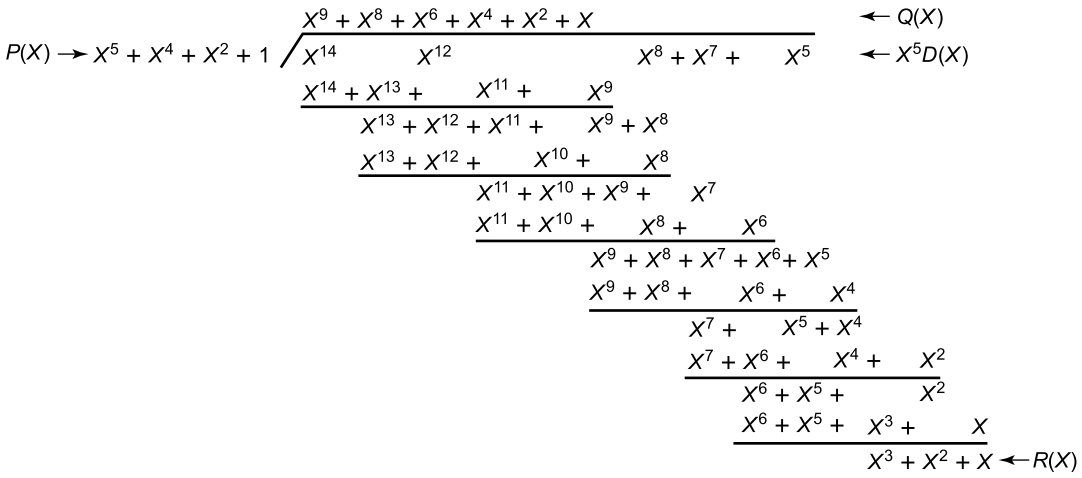


Figura 6.4. Ejemplo de división de polinomios.

- Se detectan todos los errores de un único bit si $P(X)$ tiene más de un término distinto de cero.
- Se detectan todos los errores dobles, siempre que $P(X)$ tenga al menos un factor con tres términos.
- Se detecta cualquier número impar de errores, siempre que $P(X)$ contenga el factor $(X + 1)$.
- Se detecta cualquier ráfaga de errores con longitud menor o igual que $n - k$. Es decir, menor o igual que la longitud de la FCS.
- Se detecta una fracción de las ráfagas de errores con longitud igual a $n - k + 1$, siendo la fracción igual a $1 - 2^{-(n-k-1)}$.
- Se detecta una fracción de las ráfagas de errores con longitudes mayores que $n - k + 1$ siendo la fracción igual a $1 - 2^{-(n-k)}$.

Es más, se puede demostrar que si todos los patrones de error son equiprobables, entonces, para una ráfaga de errores con longitud $r + 1$, la probabilidad de que no se detecte un error ($E(X)$ sea divisible entre $P(X)$) es $1/2^{r-1}$, y para ráfagas mayores, la probabilidad es $1/2^r$, donde r es la longitud de la FCS.

Es frecuente utilizar alguna de las cuatro definiciones siguientes para $P(X)$:

$$\begin{aligned}
\text{CRC-12} &= X^{12} + X^{11} + X^3 + X^2 + X + 1 \\
\text{CRC-16} &= X^{16} + X^{15} + X^2 + 1 \\
\text{CRC-CCITT} &= X^{16} + X^{12} + X^5 + 1 \\
\text{CRC-32} &= X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} \\
&\quad + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1
\end{aligned}$$

CRC-12 se utiliza para la transmisión de secuencias de caracteres de 6 bits y generará una FCS de 12 bits. Tanto CRC-16 como CRC-CCITT son habituales para los caracteres de 8 bits. Se utilizan, respectivamente, en los Estados Unidos y en Europa, si bien ambas generan una FCS de 16 bits. Esto podría parecer adecuado para la mayoría de las aplicaciones, no obstante, en algunas normas de transmisión síncrona sobre enlaces punto a punto se ha especificado CRC-32 como opcional. Además, esta misma CRC se utiliza en normas IEEE 802 para LAN.

Lógica digital

El procedimiento CRC se puede representar, y de hecho implementar, con un circuito divisor formado por puertas *exclusive-or* y un registro de desplazamiento. El registro de desplazamiento es una cadena de elementos de memoria de 1 bit. Cada elemento tiene una línea de salida que contendrá el valor actualmente almacenado, además de una línea de entrada. A instantes discretos de tiempo, establecidos por una señal de reloj, el valor almacenado en el elemento de memoria se reemplaza por el valor que se encuentre en la línea de entrada. Todo el registro utiliza una señal de reloj común, que provoca un desplazamiento de un bit a lo largo de todo el registro.

El circuito se construye de la siguiente manera:

1. El registro contendrá $n - k$ bits, igual a la longitud de la FCS.
2. Hay $n - k$ puertas *exclusive-or*.
3. La presencia o ausencia de puerta corresponderá con la presencia o ausencia del término correspondiente en el polinomio divisor, $P(X)$, excluyendo a los términos 1 y X^{n-k}.

Ejemplo 6.6. La arquitectura de este circuito se explica mejor considerando un caso particular, como el ejemplo que se muestra en la Figura 6.5. En este ejemplo se usa:

$$\text{Datos } D = 1010001101; \qquad D(X) = X^9 + X^7 + X^3 + X^2 + 1$$

$$\text{Divisor } P = 110101; \qquad P(X) = X^5 + X^4 + X^2 + 1$$

definidas anteriormente.

En la Figura 6.5a se muestra la realización del registro de desplazamiento. El proceso comienza con la puesta a cero de todo el registro (todo ceros). El mensaje, o dividendo, se introduce a continuación, bit a bit, comenzado por el bit más significativo. La Figura 6.5b es una tabla que muestra el funcionamiento paso a paso por cada bit de entrada. Cada fila de la tabla muestra los valores almacenados en los cinco elementos de memoria del registro de desplazamiento. Las filas muestran, además, los valores que aparecerán en las salidas de los tres circuitos *exclusive-OR*. Finalmente, en cada columna se muestra el valor del siguiente bit de entrada, disponible para el siguiente paso.

Nótese que la operación *exclusive-or* afectará a C_4, C_2 y C_0 en el siguiente desplazamiento. Esto es idéntico al procedimiento de división binaria mencionado anteriormente. El procedimiento continúa para todos los bits del mensaje. Para generar la salida se usan dos conmutadores. Los bits correspondientes a los datos de entrada se introducen poniendo los dos conmutadores a la posición *A*. A resultas, tras 10 pasos, los bits de entrada se introducirán en el registro de desplazamiento, a la vez que serán generados a la salida. Tras proceder el último bit, el registro de desplazamiento contendrá el resto (la FCS) (mostrado en cajas sombreadas). Tan pronto como el último bit de datos entra en el registro de desplazamiento, los dos conmutadores se ponen en la posición *B*. Esto causa dos efectos:

1. Todas las puertas *exclusive-or* se convierten en simples elementos de paso, es decir, no cambia ningún bit.
2. Al seguir desplazando el registro, se generarán los 5 bits correspondientes a la CRC.

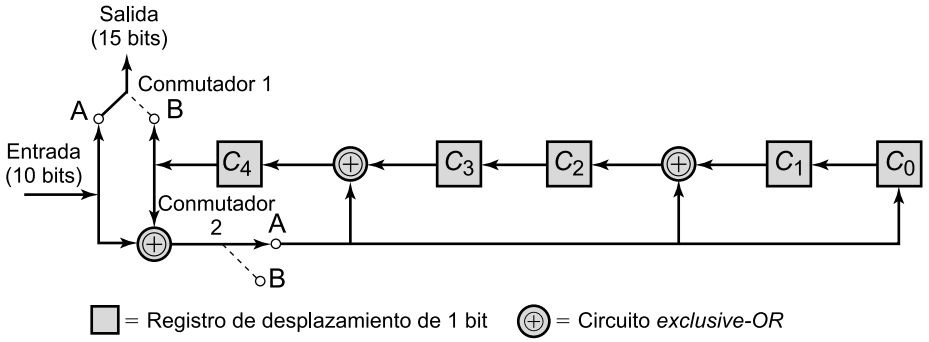
En el receptor se utiliza la misma lógica. Cada bit de un bloque de *M* se introducirá en el registro de desplazamiento. Si no ha habido errores, el registro de desplazamiento debería contener el patrón de bits *R* al final de *M*. Los bits transmitidos de *R* empiezan a llegar y el efecto consistirá en que, cuando concluya la recepción, el registro debe contener todas las posiciones igual a cero.

La Figura 6.6 muestra una arquitectura genérica para la realización de un código de CRC mediante un registro de desplazamiento para el polinomio

$$P(X) = \sum_{i=0}^{n-k} A_i X^i$$

donde $A_0 = A_{n-k} = 1$, y todos los otros A_i son iguales a 0 o 1[5].

[5] Es habitual mostrar el registro del procedimiento CRC con desplazamientos hacia la derecha, lo cual es contrario a la división binaria. Debido a que los números binarios se representan habitualmente con el bit más significativo a la izquierda, es más apropiado usar un registro de desplazamiento a la izquierda como el aquí usado.



(a) Implementación mediante registros de desplazamiento

	C_4	C_3	C_2	C_1	C_0	$C_4 \oplus C_3 \oplus I$	$C_4 \oplus C_1 \oplus I$	$C_4 \oplus I$	I = entrada	
Inicial	0	0	0	0	0	1	1	1	1	
Paso 1	1	0	1	0	1	1	1	1	0	
Paso 2	1	1	1	1	1	1	1	0	1	
Paso 3	1	1	1	1	0	0	0	1	0	
Paso 4	0	1	0	0	1	1	0	0	0	Mensaje
Paso 5	1	0	0	1	0	1	0	1	0	a enviar
Paso 6	1	0	0	0	1	0	0	0	1	
Paso 7	0	0	0	1	0	1	0	1	1	
Paso 8	1	0	0	0	1	1	1	1	0	
Paso 9	1	0	1	1	1	0	1	0	1	
Paso 10	0	1	1	1	0					

(b) Ejemplo con entrada 1010001101

Figura 6.5. Circuito con registros de desplazamiento para dividir entre el polinomio $X^5 + X^4 + X^2 + 1$.

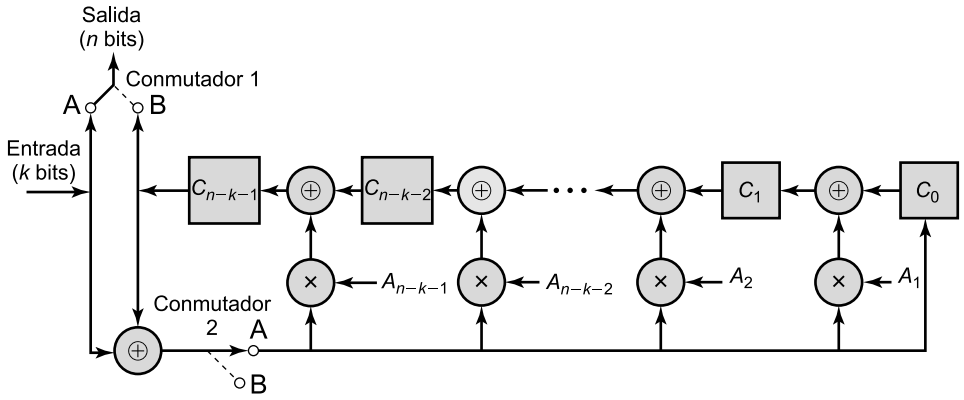


Figura 6.6. Arquitectura genérica de una CRC para implementar la división entre $(1 + A_1X + A_2X^2 + \cdots + A_{n-1}X^{n-k-1} + X^{n-k})$.

6.4. CORRECCIÓN DE ERRORES

La detección de errores es una técnica útil, incorporada en la mayoría de los protocolos de control del enlace, como por ejemplo HDLC, al igual que en los protocolos de transporte, como por ejemplo TCP. No obstante, la corrección de errores mediante el uso de códigos para la detección de

errores exige retransmitir, como se explicará posteriormente en el Capítulo 7, bloques de datos. Este enfoque puede no ser del todo apropiado en aplicaciones inalámbricas por las dos razones siguientes:

1. La tasa de errores por bit en un enlace inalámbrico puede ser bastante elevada, lo que resultará en un gran número de retransmisiones.
2. En algunos casos, especialmente en enlaces satelitales, el retardo de propagación es muy elevado, comparado con el tiempo de transmisión de la trama. Como consecuencia, se obtiene un sistema muy poco eficaz. Como se estudiará en el Capítulo 7, la aproximación más habitual es retransmitir la trama errónea además de las tramas siguientes. En enlaces de datos de gran longitud, un error en una trama aislada requerirá, por tanto, la retransmisión de muchas tramas.

En su lugar, sería deseable habilitar al receptor para que fuera capaz de corregir errores usando exclusivamente los bits recibidos en la transmisión. En la Figura 6.7 se muestra, en términos genéricos, cómo llevar a cabo este procedimiento. En el extremo del emisor, usando un codificador con corrección de errores hacia delante FEC (*Forward Error Correction*), para cada bloque de datos de k bits se genera uno de n bits ($n > k$) denominado **palabra-código,** que es transmitido. Durante la transmisión, la señal es susceptible de ser afectada por diversos contratiempos, los cuales pueden producir errores en los bits de la señal. En el receptor, la señal de entrada se demodula para obtener una cadena de bits similar a la palabra-código original, pero posiblemente con errores. Este bloque se pasa al decodificador FEC, el cual generará una de las siguientes cuatro salidas:

1. Si no ha habido errores, la entrada al decodificador FEC es idéntica a la palabra-código original, por lo que el decodificador generará el bloque de datos original.
2. Para ciertos patrones de error, es posible que el decodificador detecte y corrija esos errores. Por tanto, aunque los bloques de datos recibidos difieran de la palabra-código transmitida, el decodificador FEC será capaz de asociar el bloque recibido al bloque de datos original.

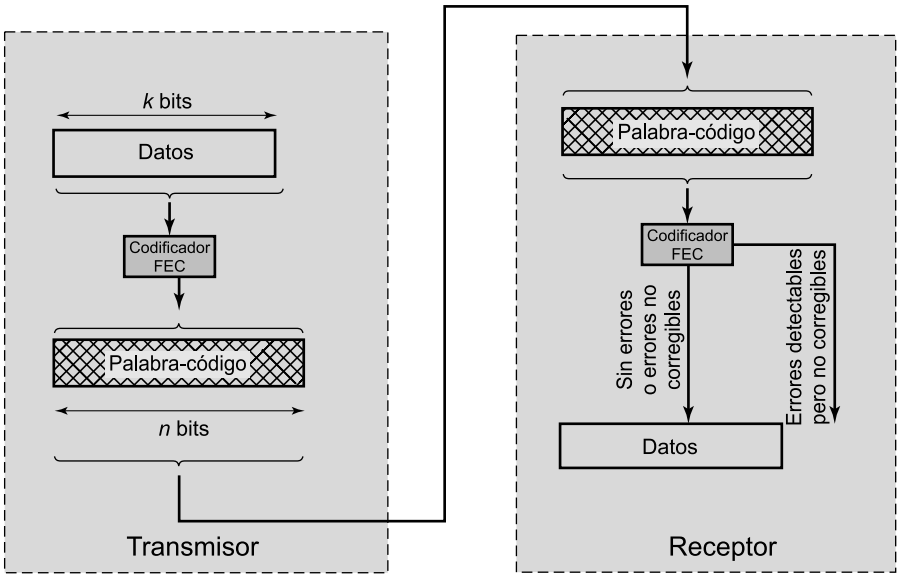


Figura 6.7. Procedimiento para corregir errores.

3. Para ciertos patrones de error, el decodificador podrá detectarlos pero no corregirlos. En este caso, el decodificador simplemente informará sobre la detección de un error irrecuperable.
4. Para ciertos, aunque raros, patrones de error, el decodificador no detectará la ocurrencia de dichos errores y asignará el bloque de datos recibido, de n bits, a un bloque de k bits que será distinto al bloque original de k bits.

¿Cómo es posible que el decodificador corrija los bits erróneos? Esencialmente, la corrección de errores funciona añadiendo redundancia al mensaje transmitido. La redundancia hace posible que el receptor deduzca cuál fue el mensaje original, incluso para ciertos niveles de la tasa de bits erróneos. En este apartado se estudia un tipo de códigos de corrección de errores denominados códigos de bloque. Nuestro estudio sólo abordará los principios básicos, ya que una discusión más detallada de los códigos de corrección está fuera de los objetivos del presente texto.

Antes de proceder, nótese que en muchos casos los códigos de corrección de errores siguen el mismo esquema que el mostrado en la Figura 6.3. Es decir, un algoritmo FEC toma como entrada un bloque de k bits, le añade $(n - k)$ bits de comprobación, generando un bloque de n bits. Todos los k bits del bloque original aparecerán en el bloque de salida de n bits. En algunos algoritmos FEC, los k bits de entrada se asignan a una palabra-código de n bits, de forma tal que los k bits de entrada no aparecen en los de salida.

PRINCIPIOS GENERALES DE LOS CÓDIGOS DE BLOQUE

Para empezar, definamos un concepto que va a ser de utilidad. Se define la **distancia de Hamming** $d(\mathbf{v}_1, \mathbf{v}_2)$ entre dos palabras de n bits $\mathbf{v}_1$ y $\mathbf{v}_2$, como el número de bits en el que $\mathbf{v}_1$ y $\mathbf{v}_2$ difieren. Por ejemplo, si

$$\mathbf{v}_1 = 011011, \qquad \mathbf{v}_2 = 110001$$

entonces

$$d(\mathbf{v}_1, \mathbf{v}_2) = 3$$

Considérese ahora una técnica de código de bloque para corregir errores. Supóngase que se quiere transmitir un bloque de datos con longitud k bits. En lugar de transmitir cada bloque de k bits, se signa cada secuencia de entrada a una única palabra-código de n bits.

Ejemplo 6.7. Para $k = 2$ y $n = 5$ se pueden realizar las siguientes asignaciones:

Bloque de datos	Palabra-código
00	00000
01	00111
10	11001
11	11110

Ahora, supóngase que se recibe una palabra-código con el patrón de bits 00100. Ésta no es una palabra-código válida, por lo que el receptor detecta un error. ¿Puede ese error ser corregido? No es posible asegurar qué bloque de datos fue transmitido ya que el ruido puede haber corrompido 1, 2, 3, 4, o incluso los 5 bits. Sin embargo, nótese que para convertir la palabra-código 00000 en 00100 sólo se necesita alterar un bit. Para transformar 00111 en 00100 se necesitarían

dos cambios, tres para transformar 11110 en 00100 y cuatro para transformar 11001 en 00100. Así, se puede deducir que la palabra-código enviada más probable fue 00000 y que, por tanto, el bloque de datos recibido es 00. Esto es básicamente una corrección de errores. En términos de la distancia de Hamming, se tiene que

$$d(00000, 00100) = 1; \quad d(00111, 00100) = 2;$$
$$d(11001, 00100) = 4; \quad d(11110, 00100) = 3$$

Por tanto, la regla a imponer sería que si se recibe una palabra-código inválida, entonces se selecciona la palabra-código válida más cercana (a distancia mínima). Esto funcionará sólo si hay una única palabra-código a la distancia mínima para cada palabra inválida.

En nuestro ejemplo, no es cierto que para todas las palabras-código inválidas haya una y solamente una palabra-código a la mínima distancia. Hay $2^5 = 32$ posibles palabras-código de las que sólo 4 son válidas, quedando 28 palabras-código inválidas. Para las palabras-código inválidas, se tiene lo siguiente:

Palabra-código inválida	Distancia mínima	Palabra-código válida	Palabra-código inválida	Distancia mínima	Palabra-código válida
00001	1	00000	10000	1	00000
00010	1	00000	10001	1	11001
00011	1	00111	10010	2	00000 o 11110
00100	1	00000	10011	2	00111 o 11001
00101	1	00111	10100	2	00000 o 11110
00110	1	00111	10101	2	00111 o 11001
01000	1	00000	10110	1	11110
01001	1	11001	10111	1	00111
01010	2	00000 o 11110	11000	1	11001
01011	2	00111 o 11001	11010	1	11110
01100	2	00000 o 11110	11011	1	11001
01101	2	00111 o 11001	11100	1	11110
01110	1	11110	11101	1	11001
01111	1	00111	11111	1	11110

Hay ocho casos en los que una palabra-código inválida está a distancia 2 de dos palabras-código válidas diferentes. Así, si se recibiera una de ésas, un error en 2 bits podría haberla generado, en este caso, el receptor no tendría forma de elegir entre las dos alternativas. Aquí se detectaría un error pero no se corregiría. No obstante, en cualquier caso en el que haya un error simple, la palabra-código resultante estaría a distancia 1 de sólo una palabra-código válida, por lo que la decisión se podría tomar fácilmente. Este código es, por tanto, capaz de corregir todos los errores simples pero no puede corregir los errores dobles. Otra forma de enfocar el problema es considerar las distancias entre las parejas de palabras-código válidas

$$d(00000, 00111) = 3; \quad d(00000, 11001) = 3; \quad d(00000, 11110) = 4;$$
$$d(00111, 11001) = 4; \quad d(00111, 11110) = 3; \quad d(11001, 11110) = 3;$$

La distancia mínima entre las palabras-código válidas es 3. Por tanto, un error en un bit dará lugar a una palabra-código inválida que está a distancia 1 de la palabra-código válida, pero al menos a distancia 2 de cualquiera de las otras palabras-código válidas. A resultas, este código siempre corrige cualquier error simple. Nótese que el código también detectará cualquier error doble.

Los ejemplos anteriores muestran las propiedades esenciales de un código de bloque de corrección de errores. Un código de bloque (n, k) codifica k bits de datos en palabras-código de n bits. Generalmente, cada palabra-código válida incluye a los k bits de datos originales y les añade $(n - k)$ bits de comprobación para constituir la palabra-código de n bits. Así, diseñar un código de bloque es equivalente a diseñar una función del tipo $\mathbf{v_c} = f(\mathbf{v_d})$, siendo $\mathbf{v_d}$ el vector de k bits de datos y $\mathbf{v_c}$ el vector de n bits correspondiente a la palabra-código.

Si se tiene un código de bloque (n, k), habrá 2^k palabras-código válidas de un total de 2^n posibles. Se define la **redundancia** del código como el cociente del número de bits redundantes entre el número de bits de datos $(n - k)/k$, y se define la **tasa** del código como el cociente del número de bits de datos entre el número de bits totales, k/n. La tasa del código es una medida del ancho de banda adicional que se necesita para transmitir los datos a la misma velocidad que si no hubiera código. Por ejemplo, para transmitir a la misma velocidad, un código cuya tasa sea $1/2$ necesitará el doble de capacidad de transmisión que un sistema que no utilice código. En el código de nuestro ejemplo, la tasa es igual a $2/5$ y, por tanto, necesita una capacidad 2,5 veces la de un sistema sin codificación. Por ejemplo, si la velocidad de transmisión de los datos a la entrada del codificador es de 1 Mbps, entonces la salida del codificador debe ser igual a 2,5 Mbps.

Para un código constituido por las palabras-código $\mathbf{w}_1$, $\mathbf{w}_2$, ..., $\mathbf{w}_s$, en el que $s = 2^k$, se define la distancia mínima del código, $d_{\min}$ como

$$d_{\min} = \min_{i \neq j} [(\mathbf{w}_i, \mathbf{w}_j)]$$

Se puede demostrar que se cumplen las siguientes afirmaciones. Dado un número entero positivo t, si el código satisface que $d_{\min} \geqslant 2t + 1$, entonces el código puede corregir todos los errores de hasta t bits. Si $d_{\min} \geqslant 2t$, entonces el código corregirá todos los errores de hasta $\leqslant t - 1$ bits y detectará los de t bits, si bien, en general no podrá corregirlos. De manera inversa, cualquier código que corrija todos los errores de hasta $\leqslant t$ bits debe verificar que $d_{\min} \geqslant 2t + 1$, y cualquier código que corrija cualquier número de bits erróneos menor o igual que $t - 1$ y que detecte todos los errores de t bits debe verificar que $d_{\min} \geqslant 2t$.

Otra forma alternativa de expresar la relación entre $d_{\min}$ y t consiste en decir que el número máximo de errores que se pueden corregir con garantías por palabra-código verifica que

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

donde $\lfloor x \rfloor$ denota al mayor entero que no es mayor que x (es decir, por ejemplo $\lfloor 6{,}3 \rfloor = 6$. Es más, si lo que interesa es sólo detectar errores y no corregirlos, entonces, el número de errores t que se pueden detectar, verifica que

$$t = d_{\min} - 1$$

Para aclarar esto, nótese que si se dan $d_{\min}$ errores, cualquier palabra-código puede convertirse en otra válida. Cualquier número menor que $d_{\min}$ errores nunca convertirá una palabra-código válida en otra válida.

El diseño de los códigos de bloque implica las siguientes consideraciones:

1. Dados unos valores n y k, sería deseable obtener el valor mayor posible de $d_{\min}$.
2. El código debería ser relativamente fácil de codificar y decodificar, con requisitos mínimos de memoria y tiempo de procesamiento.

3. Sería deseable que el número de bits redundantes, $(n - k)$, sea pequeño para reducir el ancho de banda.
4. Sería deseable que el número de bits redundantes, $(n - k)$, sea grande para reducir la tasa de errores.

Evidentemente, los dos objetivos finales son contradictorios entre sí, por lo que hay que buscar un compromiso entre ambos.

Puede ser ilustrativo examinar la Figura 6.8, basada en una de [LEBO98]. En la bibliografía relativa a los códigos de corrección de errores, se suelen incluir gráficos de este tipo para demostrar la eficacia de los distintos esquemas considerados. Recuérdese del Capítulo 5 que con la codificación se puede reducir el valor E_b/N_0 para conseguir una tasa de errores dada[6]. Los esquemas de codificación considerados en el Capítulo 5 estaban relacionados con la definición de los elementos de señalización necesarios para representar los bits. Los esquemas estudiados en este capítulo también afectan al valor E_b/N_0. En la Figura 6.8, la curva de la derecha corresponde a un sistema de modulación no codificado. La región sombreada representa el área en la que se pueden obtener mejoras. En esta región se consigue una BER (tasa de errores por bit) más pequeña para un E_b/N_0 dado, o dicho de otra forma, para una BER dada, se necesita un E_b/N_0 menor. La otra curva corresponde a un sistema típico de codificación con una tasa igual a un medio (igual número de bits de datos que de comprobación). Nótese que, para una tasa de errores igual a 10^{-5}, si se utiliza codificación, se obtiene una reducción en el valor de E_b/N_0 de 2,77 dB. Esta reducción se denomina **ganancia del código** y se define como la reducción, en decibelios, en el valor E_b/N_0 necesario para conseguir una BER dada en un sistema de codificación para corrección de errores comparada con un sistema no codificado que utilizara el mismo esquema de modulación.

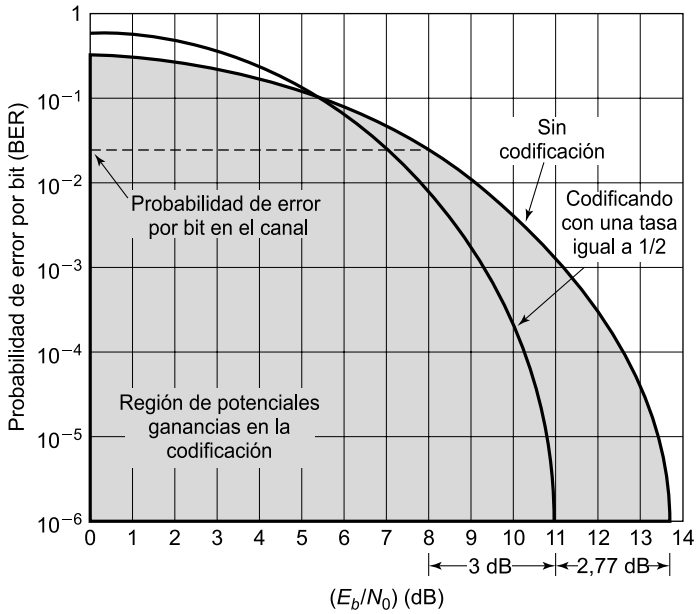


Figura 6.8. Mejoras en las prestaciones del sistema al usar codificación.

[6] E_b/N_0 es el cociente de la energía de la señal por bit entre la densidad de potencia del ruido por hercio; definida y estudiada en el Capítulo 3.

Es importante resaltar que la BER para la segunda curva (con tasa 1/2) alude a la tasa de errores no corregidos y que el valor E_b se refiere a la energía por bit. Como la tasa es igual a 1/2, en el canal habrá dos bits por cada bit de entrada al codificador, por lo que la energía por bit codificado será la mitad de la energía por bit de datos, es decir, una reducción de 3 dB. Si se considera la energía por bit de este sistema, se observa que la tasa de errores por bit del canal es $2{,}4 \times 10^{-2}$, o lo que es lo mismo, 0,024.

Finalmente, nótese que por debajo de cierto umbral para E_b/E_0, el esquema de codificación en realidad lo que hace es degradar las prestaciones. En nuestro ejemplo de la Figura 6.8, el umbral está en torno a los 5,4 dB. Por debajo de este umbral, los bits adicionales de comprobación añaden una redundancia al sistema que reduce la energía por bit de datos, incurriendo en un incremento de los errores. Por encima de ese umbral, la potencia de corrección de errores del código compensa la reducción de E_b, consiguiendo una mejora en la ganancia del código.

6.5. CONFIGURACIONES DE LÍNEA

Las dos características que distinguen a las posibles configuraciones del enlace de datos son la topología y su funcionamiento en *half-duplex* o *full-duplex*.

TOPOLOGÍA

Con el término topología se hace referencia a la disposición física de las estaciones en el medio de transmisión. Si hay sólo dos estaciones (es decir, un terminal y un computador, o dos computadores), el enlace es punto a punto. Si hay más de dos estaciones, entonces se trata de una topología multipunto. Históricamente, los enlaces multipunto se han utilizado cuando se disponía de un computador (estación principal) y un conjunto de terminales (estaciones secundarias). Actualmente, las topologías multipunto son típicas de las redes de área local.

Las topologías tradicionales multipunto son sólo útiles cuando los terminales transmiten durante una fracción del tiempo. En la Figura 6.9 se muestran las ventajas de la configuración multipunto. Si cada terminal tuviera un enlace punto a punto hasta su computador central, éste debería tener un puerto de E/S para cada terminal conectado. También se necesitaría una línea desde cada uno de los terminales al computador central. En una configuración multipunto, el computador central sólo necesita un puerto de E/S y una única línea de transmisión, ahorrando así los costes correspondientes.

FULL-DUPLEX Y *HALF-DUPLEX*

El intercambio de datos a través de una línea de transmisión se puede clasificar como *full-duplex* o *half-duplex*. En la **transmisión *half-duplex*** sólo una de las dos estaciones del enlace punto a punto puede transmitir cada vez. Este modo también se denomina *en dos sentidos alternos*, aludiendo al hecho de que las dos estaciones pueden transmitir alternativamente. Esto es comparable a un puente que tuviera un sólo carril y con circulación en los dos sentidos. Este tipo de transmisión se usa, a menudo, en la interacción entre los terminales y su computador central. Mientras que el usuario introduce y transmite datos, el computador central no podrá enviar datos al terminal, ya que si no, éstos aparecerían en la pantalla del terminal provocando confusión.

En la **transmisión *full-duplex*** las dos estaciones pueden simultáneamente enviar y recibir datos. Este modo, denominado *dos sentidos simultáneos*, es comparable a un puente que tuviera

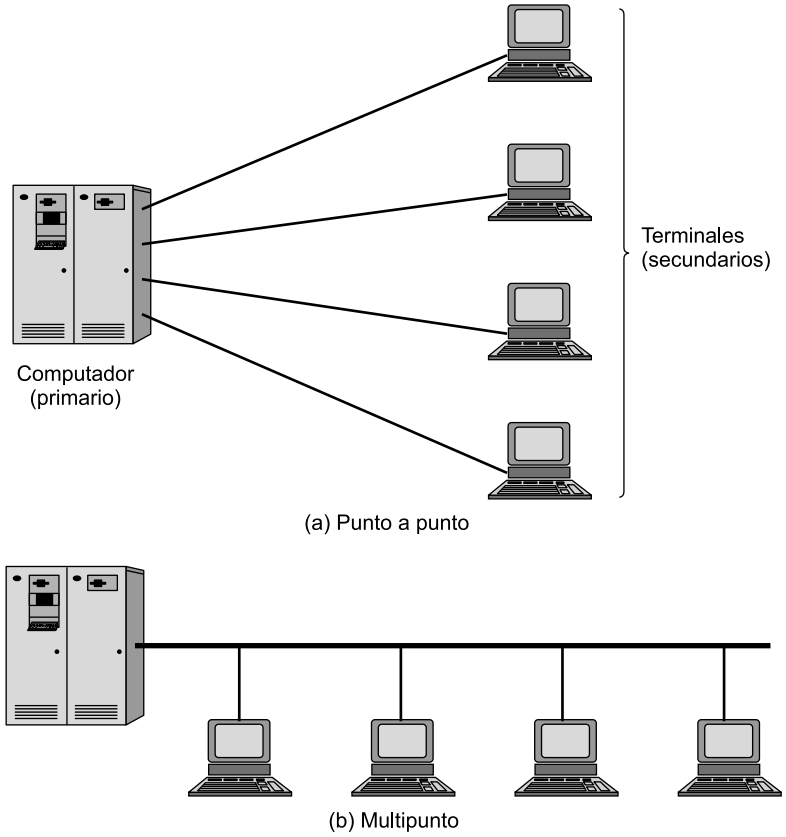


Figura 6.9. Configuraciones tradicionales computador/terminal.

dos carriles con tráfico en ambos sentidos. Para el intercambio de datos entre computadores, este tipo de transmisión es más eficiente que la transmisión *half-duplex*.

En el caso de señalización digital, en la que se requiere un medio guiado, la transmisión *full-duplex* normalmente exige dos caminos separados (por ejemplo, dos pares trenzados), mientras que la transmisión *half-duplex* necesita solamente uno. En el caso de señalización analógica, dependerá de la frecuencia: si una estación transmite y recibe a la misma frecuencia, utilizando transmisión inalámbrica se deberá operar en modo *half-duplex*, aunque para medios guiados se puede operar en *full-duplex* utilizando dos líneas de transmisión distintas. Si una estación emite en una frecuencia y recibe a otra, podrá operar en *full-duplex* si se usa transmisión inalámbrica. En el caso de medios guiados podrá operar en *full-duplex* usando una sola línea.

En realidad, es factible transmitir simultáneamente en ambas direcciones sobre una única línea de transmisión si se utiliza la técnica denominada cancelación de eco. Ésta es una técnica de procesamiento de señales cuya explicación está fuera del alcance de este texto.

6.6. INTERFACES

La mayoría de los dispositivos utilizados para el procesamiento de datos tienen una capacidad limitada de transmisión. Normalmente, generan una señal digital, como por ejemplo NRZ-L, pudiendo transmitir a una distancia limitada. Consecuentemente, es extraño que dichos dispositivos

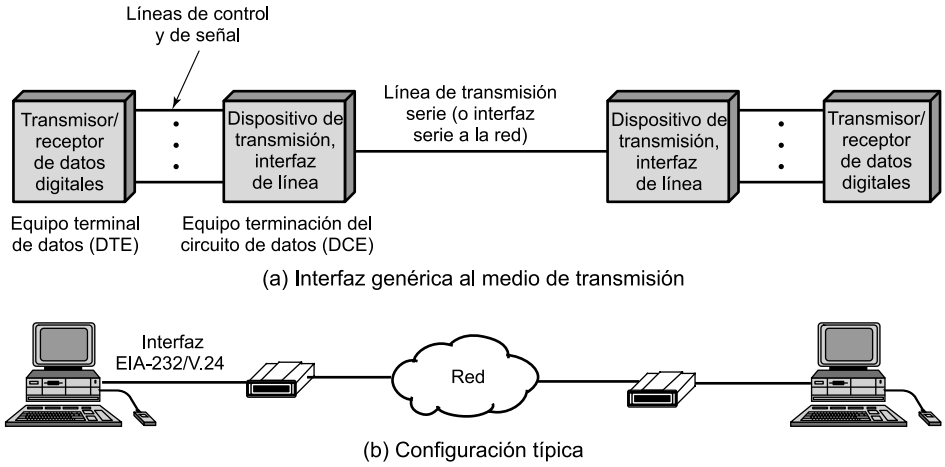


Figura 6.10. Interfaces para las comunicaciones de datos.

(terminales y computadores) se conecten directamente a la red de transmisión. En la Figura 6.10 se muestra la configuración más habitual. Los dispositivos finales, normalmente terminales y computadores, se denominan generalmente **equipo terminal de datos** (DTE, *Data Terminal Equipment*). El DTE accede al medio de transmisión mediante la utilización de un **equipo terminación del circuito de datos** (DCE, *Data Circuit-terminating Equipment*), como por ejemplo un módem.

Por un lado, el DCE es responsable de transmitir y recibir bits, de uno en uno, a través del medio de transmisión o red. Por el otro, el DCE debe interaccionar con el DTE. En general, esto exige que se intercambien tanto datos como información de control. Esto se lleva a cabo a través de un conjunto de cables que se denominan **circuitos de intercambio**. Para que este esquema funcione se necesita un alto grado de cooperación. Los dos DCE que intercambian señales a través de la línea de transmisión o la red deben entenderse mutuamente. Es decir, el receptor de cada DCE debe usar el mismo esquema de codificación (por ejemplo Manchester o PSK) y la misma velocidad de transmisión que el transmisor del otro extremo. Además, cada pareja DTE-DCE se debe diseñar para que funcione cooperativamente. Para facilitar las cosas, tanto a los usuarios como a los fabricantes de los equipos para el procesamiento de datos, se han desarrollado normalizaciones que especifican exactamente la naturaleza de la interfaz entre el DTE y el DCE. La interfaz tiene cuatro características importantes o especificaciones:

- Mecánicas.
- Eléctricas.
- Funcionales.
- De procedimiento.

Las *características mecánicas* describen la conexión física entre el DTE y el DCE. Normalmente, los circuitos de intercambio de control y de datos se embuten en un cable con un conector, macho o hembra, a cada extremo. El DTE y el DCE deben tener conectores de distinto género a cada extremo del cable. Esta configuración es análoga a los cables de suministro de energía eléctrica. La energía se facilita a través de una toma de corriente o enchufe y el dispositivo que se conecte debe tener el conector macho que corresponda a la toma (con dos polos, dos polos con polaridad o tres polos).

Las *características eléctricas* están relacionadas con los niveles de tensión y su temporización. Tanto el DTE como el DCE deben usar el mismo código (por ejemplo NRZ-L), deben usar los mismos niveles de tensión y deben utilizar la misma duración para los elementos de señal. Estas características determinan la velocidad de transmisión, así como las máximas distancias que se puedan conseguir.

Las *características funcionales* especifican las funciones que se realizan a través de cada uno de los circuitos de intercambio. Las funciones a realizar se pueden clasificar en cuatro grandes categorías: datos, control, temporización y masa o tierra.

Las *características de procedimiento* especifican la secuencia de eventos que se deben dar en la transmisión de los datos, basándose en las características funcionales de la interfaz. Los ejemplos que se explican a continuación pueden clarificar este concepto.

Existen varias normalizaciones para la interfaz. En esta sección se presentan dos de las más significativas: V.24/EIA-232-F y la interfaz física de RDSI.

V.24/EIA-232-F

La interfaz que más se utiliza es la especificada en el estándar V.24 de la UIT-T. De hecho, este estándar especifica sólo los aspectos funcionales y de procedimiento de la interfaz; para definir los aspectos eléctricos y mecánicos hace referencia a otros estándares. En los Estados Unidos se define la norma EIA-232-F, una especificación prácticamente idéntica a V.24 que cubre las cuatro características mencionadas. La correspondencia es la siguiente:

- Mecánicas: ISO 2110
- Eléctricas: V.28
- Funcionales: V.24
- De procedimiento: V.24

EIA-232 se definió inicialmente como RS-232 por la EIA (*Electronic Industries Alliance*) en 1962. Actualmente está en su sexta versión, EIA-232-F, establecida en 1997. Las versiones actuales de V.24 y V.28 se establecieron en 1996 y 1993 respectivamente. Esta interfaz se utiliza para la conexión de los dispositivos DTE a los módem, que a su vez están conectados a líneas de calidad telefónica en sistemas analógicos públicos de telecomunicación. También se utiliza en otras muchas aplicaciones de interconexión.

Especificaciones mecánicas

En la Figura 6.11 se muestran las especificaciones mecánicas de EIA-232-F. Se usa un conector de 25 contactos distribuidos de una manera específica, según se define en la norma ISO 2110. Este conector es el terminador del cable que va desde el DTE (el terminal) al DCE (por ejemplo, el módem). Por tanto, en teoría habría que utilizar un cable que tuviera 25 conductores, aunque en la mayoría de las aplicaciones prácticas se usa un número menor de circuitos y, por tanto, de conductores.

Especificaciones eléctricas

Aquí se define la señalización entre el DTE y el DCE. Se utiliza señalización digital en todos los circuitos de intercambio. Dependiendo de la funcionalidad del circuito de intercambio, los valores

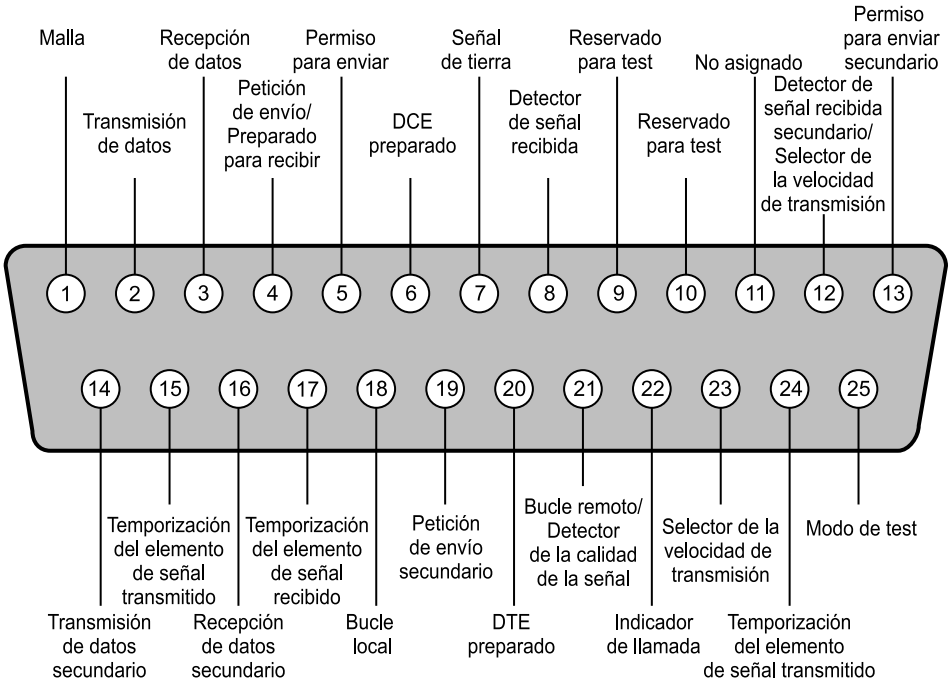

Malla
Recepción de datos
Permiso para enviar
Señal de tierra
Reservado para test
No asignado
Permiso para enviar secundario
Transmisión de datos
Petición de envío/ Preparado para recibir
DCE preparado
Detector de señal recibida
Reservado para test
Detector de señal recibida secundario/ Selector de la velocidad de transmisión
1 2 3 4 5 6 7 8 9 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25
Temporización del elemento de señal transmitido
Temporización del elemento de señal recibido
Petición de envío secundario
Bucle remoto/ Detector de la calidad de la señal
Selector de la velocidad de transmisión
Modo de test
Transmisión de datos secundario
Recepción de datos secundario
Bucle local
DTE preparado
Indicador de llamada
Temporización del elemento de señal transmitido

Figura 6.11. Asignación de los terminales en V.24/EIA-232 (conector en el DTE).

eléctricos se interpretarán como datos binarios o como señales de control. Esta normalización especifica que, respecto a una referencia de tierra común, una tensión más negativa que -3 voltios se interprete como un 1 binario, mientras que una tensión mayor de $+3$ voltios se interprete como un 0 binario. Esto corresponde al código NRZ-L mostrado en la Figura 5.2. La interfaz se utiliza a una velocidad de transmisión menor de 20 kbps para cubrir distancias menores que 15 metros. Con un diseño adecuado se pueden conseguir distancias y velocidades mayores, pero es prudente suponer que estos límites deben respetarse tanto en teoría como en la práctica.

Para las señales de control se aplican los mismos niveles de tensión: una tensión menor de -3 voltios se interpreta como OFF y una tensión mayor de $+3$ voltios se interpreta como ON.

Especificaciones funcionales

En la Tabla 6.1 se resumen las especificaciones funcionales de los circuitos de intercambio y en la Figura 6.11 se muestra la localización de estos circuitos en el conector. Los circuitos se pueden clasificar en datos, control, temporización y tierra. Hay un circuito en cada dirección, por lo que es posible el funcionamiento *full-duplex*. Es más, hay dos circuitos de datos secundarios que son útiles cuando el dispositivo funciona en *half-duplex*. En el caso de funcionamiento *half-duplex*, el intercambio de datos entre dos DTE (a través de sus DCE y el enlace de comunicaciones correspondiente) se realiza en un instante dado en una única dirección. No obstante, puede que en un momento dado se necesite enviar una petición de parada o un mensaje de control de flujo al dispositivo transmisor. Para llevar a cabo esta funcionalidad, el enlace de comunicaciones se dota de un canal en sentido inverso, normalmente a una velocidad de transmisión muy inferior que el canal primario. En la interfaz DTE-DCE el canal en sentido inverso se establece en una pareja de circuitos de datos independientes.

Tabla 6.1. Circuitos de intercambio en V.24/EIA-232-F.

V.24	EIA-232	Nombre	Dirección hacia:	Función
		SEÑALES DE DATOS		
103	BA	Transmisión de datos	DCE	Transmitidos por DTE
104	BB	Recepción de datos	DTE	Recibidos por el DTE
118	SBA	Transmisión de datos secundario	DCE	Transmitidos por DTE
119	SBB	Recepción de datos secundario	DTE	Recibidos por el DTE
		SEÑALES DE CONTROL		
105	CA	Petición de envío	DCE	El DTE desea transmitir
106	CB	Preparado para enviar	DTE	El DCE está preparado para recibir; respuesta a la petición de envío
107	CC	DCE preparado	DTE	El DCE está preparado para funcionar
108.2	CD	DTE preparado	DCE	El DTE está preparado para funcionar
125	CE	Indicador de llamada	DTE	El DCE está recibiendo la señal de llamada
109	CF	Detector de señal recibida	DTE	El DCE está recibiendo una señal dentro de los límites apropiados por la línea
110	CG	Detector de señal de calidad	DTE	Indica si la probabilidad de error es alta en los datos recibidos
111	CH	Selector de la velocidad de transmisión de la señal	DCE	Selecciona una de entre dos velocidades de transmisión
112	CI	Selector de la velocidad de transmisión de la señal	DTE	Selecciona una de entre dos velocidades de transmisión
133	CJ	Preparado para recibir	DCE	Control de flujo ON/OFF
120	SCA	Petición de envío secundaria	DCE	El DTE desea transmitir en el canal reverso
121	SCB	Preparado para enviar secundario	DTE	El DCE está preparado para recibir por el canal reverso
122	SCF	Detector de señal recibida secundario	DTE	Igual que el 109, pero por el canal reverso
140	RL	Bucle remoto	DCE	Solicita al DCE remoto que devuelva las señales recibidas
141	LL	Bucle local	DCE	Solicita al DCE que devuelva las señales recibidas
142	TM	Modo de test	DTE	El DCE se pone en modo de test
		SEÑALES DE TEMPORIZACIÓN		
113	DA	Temporización del elemento de señal transmitido	DCE	Señal de reloj: aparecen transiciones a ON y OFF en el centro de cada elemento de señal
114	DB	Temporización del elemento de señal transmitido	DTE	Señal de reloj: tanto el 113 como el 114 están relacionados con la señal del circuito 103
115	DD	Temporización del elemento de señal recibido	DTE	Señal de reloj para el circuito 104
		TIERRA		
102	AB	Señal de tierra/retorno		Referencia de tierra común para todos los circuitos

Hay 16 circuitos de control. Los 10 primeros, relacionados con la transmisión de datos sobre el canal primario, se listan en la Tabla 6.1. En el caso de transmisión asíncrona, se utilizan seis de estos circuitos (105, 106, 107, 108.2, 125, 109). La utilización de estos circuitos se explica en la subsección relativa a las especificaciones de procedimiento. Además de estos seis circuitos, en la transmisión síncrona se utilizan otros tres circuitos de control. El circuito detector de la calidad de la señal (*Signal Quality Detector*) se pone a ON por el DCE para indicar que la calidad de la señal de entrada a través de la línea telefónica se ha deteriorado por encima de un umbral predefinido. La mayoría de los módem de alta velocidad admiten más de una velocidad de transmisión, por lo que si la línea se vuelve ruidosa pueden solicitar una reducción de la velocidad de transmisión. Los circuitos de selección de la velocidad de transmisión (*Data Signal Rate Detector*) se utilizan para cambiar de velocidad; tanto el DTE como el DCE pueden iniciar la modificación. El circuito 133 habilita al receptor para que habilite o deshabilite el flujo de datos en el circuito 104. Los tres siguientes circuitos de control (120, 121, 122) se utilizan para controlar el uso del canal secundario, el cual puede ser utilizado como canal de sentido inverso o para algún otro propósito auxiliar.

El último grupo de señales de control está relacionado con la verificación o test de la conexión entre el DTE y el DCE. Estos circuitos permiten que el DTE haga que el DCE realice un test de la conexión. Estos circuitos son útiles sólo si el módem o el DTE de que se trate admite un bucle de control, si bien esto es una característica habitual en la mayoría de los módem actuales. Funcionando en bucle local, la salida del transmisor del módem se conecta con la entrada del receptor, desconectando el módem de la línea de transmisión. Al módem se le envía una cadena de datos generada por el dispositivo del usuario, la cual es devuelta posteriormente al usuario formando un bucle. En el bucle remoto, el módem local se conecta a la línea de transmisión en la forma habitual y la salida del receptor del módem remoto se conecta a la entrada del transmisor del mismo. En cualquiera de los posibles modos de test, el DCE pone a ON el circuito de modo de test. En la Tabla 6.2 se muestran los valores de todos los circuitos que están relacionados con el bucle de test y en la Figura 6.12 se explica su utilización.

Tabla 6.2. Valores de los circuitos para los bucles en V.24/EIA-232.

Bucle local		**Bucle remoto**		
Circuito	**Condición**	**Cicuito**	**Interfaz local**	**Interfaz remota**
DCE preparado	ON	DCE preparado	ON	OFF
Bucle local	ON	Bucle local	OFF	OFF
Bucle remoto	OFF	Bucle remoto	ON	OFF
Modo de test	ON	Modo de test	ON	ON

El control del bucle es una herramienta útil para el diagnóstico de fallos. Por ejemplo, supóngase que un usuario en un computador personal se comunica con un servidor mediante una conexión a través de un módem y, de pronto, la transmisión se interrumpe. El problema podría estar en el módem local, en los servicios de transmisión, en el módem remoto o en el servidor remoto. El administrador de la red podrá usar los tests para identificar el fallo. Con el test del bucle local se comprueba el funcionamiento de la interfaz local así como del DCE local. Con los tests remotos se puede comprobar el funcionamiento del canal de transmisión y del DCE remoto.

Las señales de temporización proporcionan los pulsos de reloj en la transmisión síncrona. Cuando el DCE envía datos síncronos a través del circuito de recepción de datos (104), a la vez,

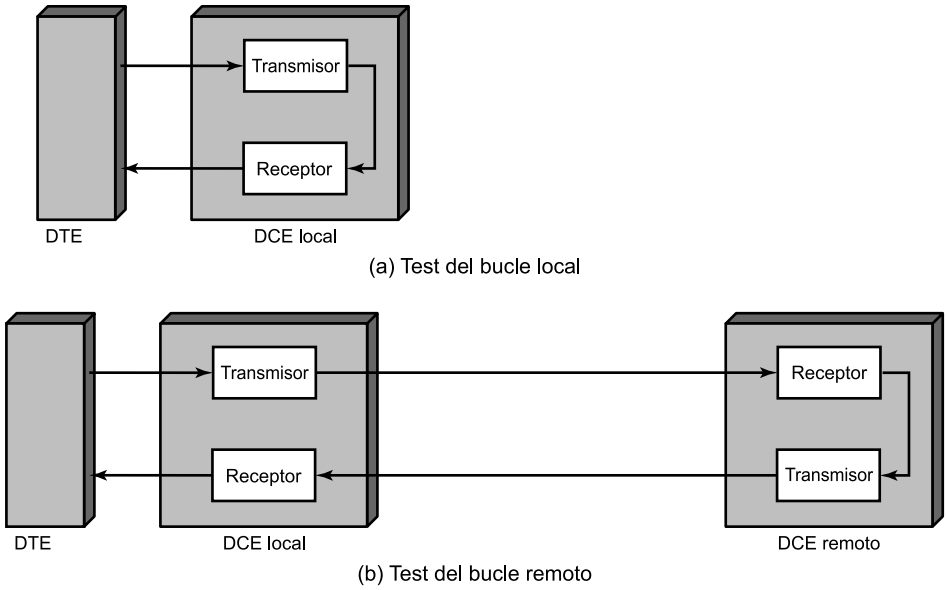


Figura 6.12. Bucles local y remoto.

envía transiciones de 0 a 1 o de 1 a 0 por el circuito de temporización del elemento de señal recibido (115), estando localizadas las transiciones en la mitad de cada elemento de señalización del circuito de recepción de datos. Cuando el DTE transmita datos síncronos, tanto el DTE como el DCE pueden proporcionar los pulsos de temporización, dependiendo de las circunstancias.

Finalmente, la señal de retorno de tierra común (102) sirve como un circuito de retorno para todos los circuitos de datos. Por tanto, la transmisión no es equilibrada, teniendo sólo un conductor activo. La transmisión equilibrada y no equilibrada se estudia en la sección dedicada a la interfaz RDSI.

Especificaciones de procedimiento

Las características de procedimiento definen la secuenciación de los diferentes circuitos en una aplicación determinada. Para tal fin, se pondrán algunos ejemplos.

El primer ejemplo es muy habitual y se trata de la conexión de dos dispositivos separados a una distancia corta dentro de un edificio. A los dispositivos en esta configuración se les denomina módem de línea privada o módem de distancia limitada. Como su propio nombre indica, los módem de distancia limitada admiten señales del DTE, como por ejemplo un terminal o un computador, las convierten a señales analógicas y las transmiten a una distancia corta a través de un medio, como por ejemplo un par trenzado. En el otro extremo de la línea hay otro módem de distancia limitada que acepta las señales analógicas de entrada, las convierte a digital y las transfiere al terminal o computador remoto. Evidentemente, se da por supuesto que el intercambio de información es en los dos sentidos. En esta aplicación se necesitan solamente los siguientes circuitos de intercambio:

- Señal de tierra (102)
- Transmisión de datos (103)

- Recepción de datos (104)
- Petición de envío (105)
- Permiso para enviar (106)
- DCE preparado (107)
- Detector de señal recibida (109)

Cuando el módem (DCE) se enciende y está preparado para funcionar, activa la línea DCE preparado (aplicando una tensión negativa y constante). Cuando el DTE está preparado para enviar datos (por ejemplo, cuando el usuario de un terminal ha introducido un carácter), activará la línea petición de envío. El módem responde, cuando esté preparado, activando el circuito permiso para enviar, e indicando que se pueden transmitir datos por la línea de transmisión de datos. Si la transmisión es *half-duplex*, el circuito de petición de envío, a su vez, inhibe el modo de recepción. El DTE puede ahora transmitir datos a través de la línea de transmisión de datos. Cuando se reciben datos del módem remoto, el módem local activa la línea detector de señal recibida para indicar que el módem remoto está transmitiendo y, además, transfiere los datos a través de la línea recepción de datos. Obsérvese que no es necesaria la utilización de circuitos de temporización, ya que se trata de transmisión asíncrona.

Los circuitos mencionados anteriormente son suficientes para los módem punto a punto sobre líneas privadas. No obstante, para transmitir datos a través de una línea de teléfono convencional se necesitan otros circuitos adicionales. En este caso, el que inicie la conexión debe llamar al destino a través de la red. Se necesitan dos circuitos adicionales:

- DTE preparado (108.2)
- Indicador de llamada (125)

Con estas dos líneas adicionales, el sistema formado por el módem y el DTE podrá usar la red telefónica de una forma análoga a como se hace en una conversación convencional. En la Figura 6.13 se muestran los pasos necesarios en una llamada *half-duplex*. Cuando se realiza la llamada, tanto manualmente como automáticamente, el sistema telefónico envía la señal de llamada. Un teléfono respondería a esta llamada haciendo sonar su timbre; un módem responde activando el circuito indicación de llamada. Una persona responde a la llamada descolgando el auricular; el DTE responde activando el circuito terminal de datos preparado. Una persona que contestara una llamada oiría la otra voz, y si no oyese nada, colgaría. Un DTE intentará monitorizar el detector de señal recibida, que será activado por el módem cuando una señal esté presente. Si este circuito no se activa, el DTE desactivará el DTE preparado. Nos podemos preguntar, ¿bajo qué circunstancias puede darse este último caso? Una situación habitual es, por ejemplo, si una persona marca accidentalmente el número de un módem. Esto activaría el DTE del módem, pero al no recibir portadora, el problema se resuelve como ya se ha indicado.

Es ilustrativo considerar la situación en la que la distancia entre los dispositivos sea tan pequeña que permita a los DTE conectarse directamente. En este caso, se pueden usar los circuitos de intercambio de la norma V.24/EIA-232, pero sin necesidad de usar DCE. Para que este esquema funcione, se necesita una configuración de módem nulo, consistente en conectar los circuitos de tal manera que se engañe a ambos DTE haciéndolos creer que están conectados a un módem. En la Figura 6.14 se muestra un ejemplo de configuración de módem nulo; el porqué de las conexiones particulares indicadas en la figura debe ser evidente para el lector que haya seguido perfectamente los razonamientos anteriores.

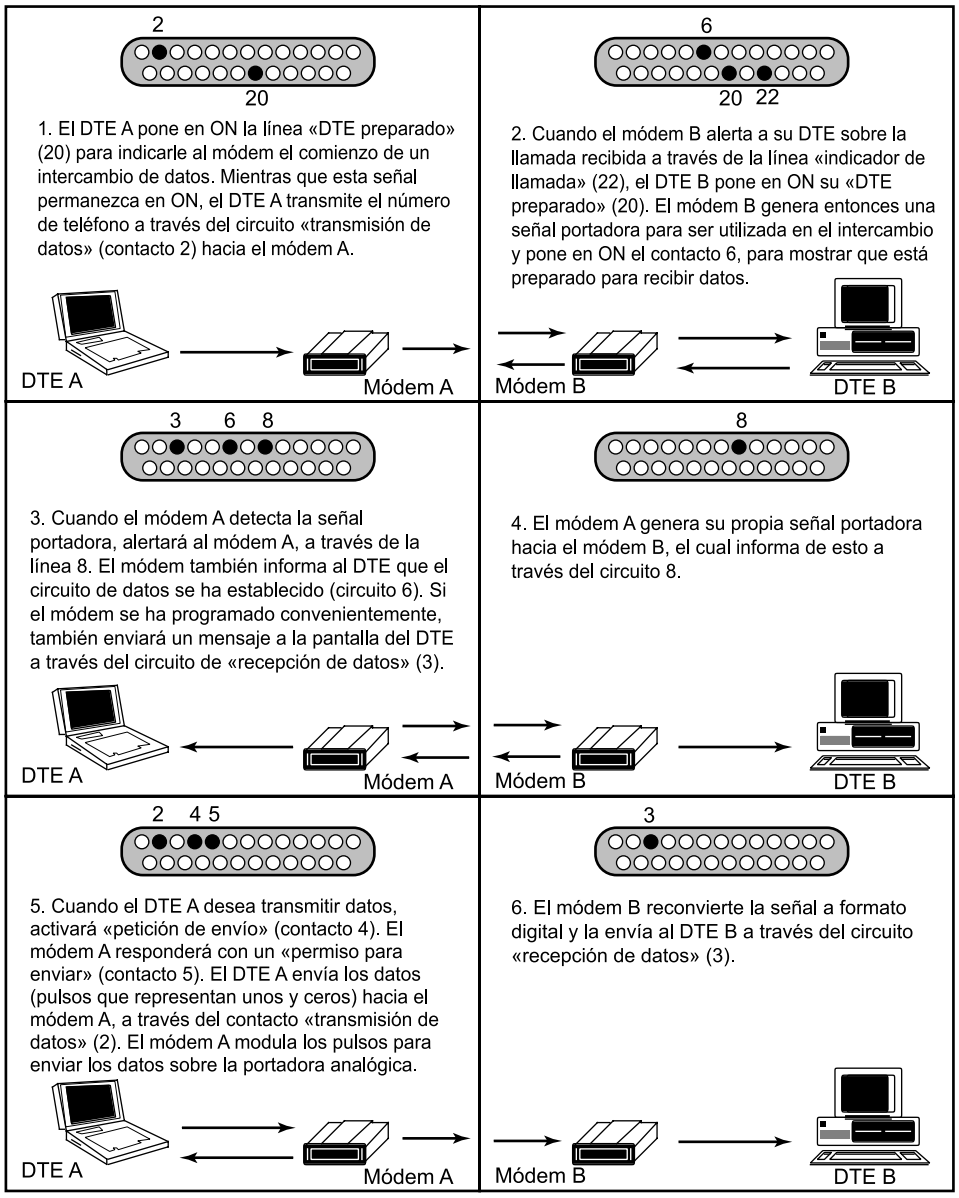

2
20
1. El DTE A pone en ON la línea «DTE preparado» (20) para indicarle al módem el comienzo de un intercambio de datos. Mientras que esta señal permanezca en ON, el DTE A transmite el número de teléfono a través del circuito «transmisión de datos» (contacto 2) hacia el módem A.
DTE A
Módem A
6
20 22
2. Cuando el módem B alerta a su DTE sobre la llamada recibida a través de la línea «indicador de llamada» (22), el DTE B pone en ON su «DTE preparado» (20). El módem B genera entonces una señal portadora para ser utilizada en el intercambio y pone en ON el contacto 6, para mostrar que está preparado para recibir datos.
Módem B
DTE B
3 6 8
3. Cuando el módem A detecta la señal portadora, alertará al módem A, a través de la línea 8. El módem también informa al DTE que el circuito de datos se ha establecido (circuito 6). Si el módem se ha programado convenientemente, también enviará un mensaje a la pantalla del DTE a través del circuito de «recepción de datos» (3).
DTE A
Módem A
8
4. El módem A genera su propia señal portadora hacia el módem B, el cual informa de esto a través del circuito 8.
Módem B
DTE B
2 4 5
5. Cuando el DTE A desea transmitir datos, activará «petición de envío» (contacto 4). El módem A responderá con un «permiso para enviar» (contacto 5). El DTE A envía los datos (pulsos que representan unos y ceros) hacia el módem A, a través del contacto «transmisión de datos» (2). El módem A modula los pulsos para enviar los datos sobre la portadora analógica.
DTE A
Módem A
3
6. El módem B reconvierte la señal a formato digital y la envía al DTE B a través del circuito «recepción de datos» (3).
Módem B
DTE B

Figura 6.13. Realización de una llamada en V.24/EIA-232..

INTERFAZ FÍSICA DE RDSI

La gran variedad de funciones que proporciona el V.24/EIA-232 se llevan a cabo mediante el uso de un gran número de circuitos de intercambio. Ésta es una solución costosa. Una alternativa sería utilizar menos circuitos incorporando más lógica de control entre las interfaces del DTE y el DCE. De esta forma se reducen los costes de circuitería, haciendo que esta aproximación sea una alternativa atractiva. Esta filosofía se adoptó en la especificación estándar X.21 (conector de 15 contactos) para la interfaz a redes públicas de conmutación de circuitos. Más recientemente, esta tendencia

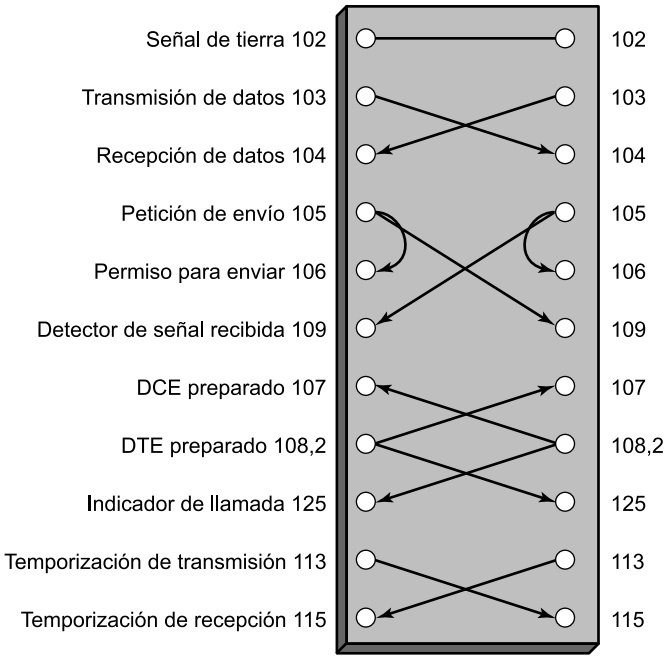


Figura 6.14. Ejemplo de un módem nulo.

se ha adoptado de forma más radical en la especificación de la Red Digital de Servicios Integrados (RDSI), en la que se define un conector con 8 contactos. La RDSI es una red completamente digital alternativa a las redes de telecomunicaciones analógicas y de telefonía pública existentes en la actualidad. En esta sección, se estudia la interfaz física definida en RDSI.

Conexión física

En la terminología RDSI, se establece una conexión física entre el equipo terminal (TE, *Terminal Equipment*) y el equipo terminador de línea (NT, *Network-Terminating equipment*). Para el estudio que aquí se va a realizar, estos dos términos son bastante análogos a los de DTE y DCE, respectivamente. La conexión física, definida en ISO 8877, especifica que los cables del NT y del TE tengan los conectores correspondientes, cada uno de ellos con 8 contactos.

En la Figura 6.15 se ilustra la asignación de estos contactos para cada una de las 8 líneas, tanto en el NT como en el TE. Para transmitir datos en cada una de las dos direcciones se usan dos terminales. Éstos se utilizan para conectar mediante pares trenzados los circuitos entre el NT y el TE. Debido a que los circuitos no tienen especificaciones funcionales específicas, los circuitos de recepción y transmisión se utilizan para transmitir tanto señales de datos como de control. La información de control se transmite usando mensajes.

Esta norma prevé la posibilidad de transmitir energía a través de la interfaz, en cualquiera de los dos sentidos, dependiendo de la aplicación en particular de que se trate. En una aplicación determinada, puede ser deseable la transferencia de energía desde la red hacia el terminal para que, por ejemplo, el servicio de telefonía básica funcione incluso en el caso de fallos del suministro eléctrico local. La transferencia de potencia se puede llevar a cabo usando los mismos cables que se usan para la transmisión de señal digital (c, d, e, f), o en los otros circuitos g, h. Los otros dos circuitos restantes no se usan en RDSI, pero pueden ser útiles en otras aplicaciones.

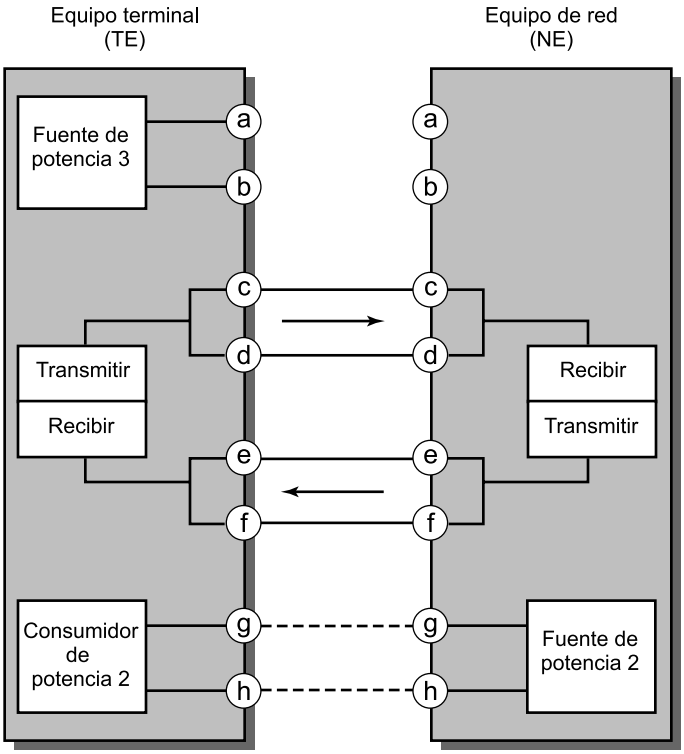


Figura 6.15. Interfaz RDSI.

Especificaciones eléctricas

La especificación eléctrica de RDSI establece que se use transmisión equilibrada. En la *transmisión equilibrada*, las señales se transmiten usando dos conductores, como por ejemplo un par trenzado. Las señales se transmiten mediante una corriente que va a través de uno de los conductores y retorna por el otro, formando un circuito cerrado. En el caso de señales digitales, esta técnica se denomina *señalización diferencial*[7], ya que los valores binarios dependen del sentido de las diferencias de tensión entre los dos conductores. La *transmisión no equilibrada* se usa en interfaces más antiguas, como la EIA-232, en la que se utiliza un solo conductor para transportar la señal, siendo el camino de retorno el circuito de tierra.

El modo equilibrado tolera más, y produce menos ruido que el modo no equilibrado. Idealmente, las interferencias en una línea equilibrada afectarán a ambos conductores por igual y no afectarán, por tanto, a las diferencias de tensión. Debido a que la transmisión no equilibrada no posee estas ventajas, su uso está normalmente restringido a cables coaxiales. Cuando se usa en circuitos de intercambio, como por ejemplo en EIA-232, las distancias son generalmente cortas.

El formato usado en la codificación de los datos en la interfaz RDSI depende de la velocidad de transmisión de los datos. Para la velocidad correspondiente a *accesos básicos* (192 kbps), el estándar especifica la utilización de codificación pseudoternaria (*véase* Figura 5.2). Los unos binarios se representan por la ausencia de tensión y el cero binario se representa por un pulso negativo

[7] No se confunda con la codificación diferencial; *véase* la Sección 5.1.

o positivo de 750 mV $\pm$ 10%. Para velocidades correspondientes a *accesos primarios*, hay dos posibilidades: si se opta por una velocidad de transmisión igual a 1.544 Mbps se utiliza la codificación con inversión de marca alternante (AMI, *Alternate Mark Inversion*) con B8ZS (*véase* Figura 5.6) y si se opta por una velocidad igual a 2.048 Mbps se utiliza la codificación AMI con HDB3. La justificación de por qué se utilizan distintos esquemas para las dos velocidades se debe a motivos históricos, ya que ninguno de los dos presenta ventajas especiales respecto al otro.

6.7. LECTURAS RECOMENDADAS

El manual clásico acerca de los códigos para la detección de errores y las técnicas de CRC es [PETE61]. [RAMA88] es un tutorial excelente sobre las CRC.

[STAL02] estudia la mayoría de los códigos para la corrección de errores. [ADAM91] proporciona un tratamiento comprensible de los códigos para la corrección de errores. [SKLA01] contiene una sección muy clara y muy bien escrita sobre el tema. Dos artículos bastante útiles son [BERL87] y [BHAR83]. Un manual matemático y teórico que se lee con facilidad puede encontrarse en [ASH90].

En [BLAC96] se lleva a cabo un estudio detallado y extenso de un gran número de normalizaciones para la interfaz a nivel físico. [BLAC95] se centra en las series V de las recomendaciones de la UIT-T. Estos temas también se abordan con cierto detalle en [FREE98].

ADAM91 Adamek, J. *Foundations of Coding*. New York: Wiley, 1991.

ASH90 Ash, R. *Information Theory*. New York: Dover, 1990.

BERL87 Berlekamp, E.; Peile, R.; y Pope, S. «The Application of Error Control to Communications.» *IEEE Communications Magazine*, abril 1987.

BHAR83 Bhargava, V. «Forward Error Correction Schemes for Digital Communications.» *IEEE Communications Magazine*, enero 1983.

BLAC95 Black, U. *The V Series Recommendations*: *Standards for Data Communications Over the Telephone Network*. New York: McGraw-Hill, 1996.

BLAC96 Black, U. *Physical Level Interfaces and Protocols*. Los Alamitos, CA: IEEE Computer Society Press, 1996.

FREE98 Freeman, R. *Telecommunication Transmission Handbook*. New York: Wiley, 1998.

PETE61 Peterson, W., y Brown, D. «Cyclic Codes for Error Detection.» *Proceedings of the IEEE*, enero 1961.

RAMA88 Ramabadran, T., y Gaitonde, S. «A Tutorial on CRC Computations.» *IEEE Micro*, agosto 1988.

SKLA01 Sklar, B. *Digital Communications*: *Fundamentals and Applications*. Upper Saddle River, NJ: Prentice Hall, 2001.

STAL02 Stallings, W. *Wireless Communications and Networks*. Upper Saddle River, NJ: Prentice Hall, 2001.

6.8. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

bit de paridad
circuitos de intercambio
código cíclico
código de Hamming
código para la corrección de errores (ECC, *Error-Correction Code*)
comprobación de paridad
comprobación de redundancia cíclica (CRC, *Cyclic Redundancy Check*)
corrección de errores
corrección de errores hacia delante (FEC, *Forward Error Correction*)
detección de errores
distancia de Hamming
EIA-232
equipo terminal de datos (DTE, *Data Terminal Equipment*)
equipo terminación del circuito de datos (DCE, *Data Circuit-terminating Equipment*)
full-duplex
half-duplex
módem
palabra-código
punto a punto
Red Digital de Servicios Integrados (RDSI)
secuencia de comprobación de trama (FCS, *Frame Check Sequence*)
trama
transmisión asíncrona
transmisión síncrona

CUESTIONES DE REPASO

6.1. En la transmisión asíncrona, ¿cómo se distingue entre la transmisión de un carácter y el siguiente?

6.2. ¿Cuál es la desventaja principal de la transmisión asíncrona?

6.3. ¿Cómo se realiza la sincronización en la transmisión síncrona?

6.4. ¿Qué es un bit de paridad?

6.5. ¿Qué es la CRC?

6.6. ¿Por qué es de esperar que una CRC detecte más errores que un bit de paridad?

6.7. Enumere tres procedimientos distintos para obtener un algoritmo de CRC.

6.8. ¿Es posible diseñar un ECC que, aun corrigiendo algunos errores dobles, no los corrija todos? ¿Por qué o por qué no?

6.9. En un ECC de bloque (n, k), ¿qué significa n y k?

6.10. ¿Qué es un DCE y cuál es su función?

EJERCICIOS

6.1. Supóngase que se envía un fichero de 10.000 bytes por una línea a 2.400 bps.

a) Calcule la redundancia, en términos de los bits suplementarios y tiempos introducidos, si se utiliza transmisión asíncrona. Suponga un bit de comienzo y un bit de parada con longitudes iguales a la de un bit de datos y suponga que por cada carácter se transmiten 8 bits sin paridad.

b) Calcule la redundancia, en términos de los bits suplementarios y tiempos introducidos, si se utiliza transmisión síncrona. Suponga que los datos se envían en tramas. Cada trama tiene 1.000 caracteres = 8.000 bits, con una cabecera de 48 bits de control por cada trama.

c) ¿Cuáles serían las repuestas para los apartados a y b si el fichero tuviera 100.000 caracteres?

d) ¿Cuáles serían las repuestas para los apartados a y b para el fichero original de 10.000 caracteres, pero a una velocidad de 9.600 bps?

6.2. Una fuente generadora de datos produce caracteres IRA de 7 bits. Obtenga una expresión para la velocidad de transmisión máxima (velocidad de transmisión de los bits de los datos IRA) para una línea de x bps en las siguientes configuraciones:

a) Transmisión asíncrona con 1,5 bits de parada y un bit de paridad.

b) Transmisión síncrona, con una trama con 48 bits de control y 128 bits de información. El campo de información contiene caracteres IRA de 8 bits (con la paridad incluida).

c) Igual que en b pero con un campo de información de 1.024 bits.

6.3. Demuestre mediante un ejemplo (escribiendo una serie de bits, considerando que los bits de comienzo y parada tienen una duración de un bit) que un receptor que comete un error en la delimitación de una trama en transmisión asíncrona puede volver a realinearse.

6.4. Supóngase que el emisor y el receptor acuerdan no usar bits de parada en una transmisión asíncrona. ¿Funcionaría la conexión? Si es así, explique las condiciones necesarias para ello.

6.5. En un esquema de transmisión asíncrona se usan 8 bits de datos, un bit de paridad par y un elemento de parada de longitud 2 bits. ¿Cuál es el porcentaje de imprecisión que se puede permitir para el reloj del receptor sin que se cometa un error en la delimitación? Supóngase que los bits se muestrean en mitad del intervalo de señalización. Supóngase también que al principio del bit de comienzo el reloj y los bits recibidos están en fase.

6.6. Supóngase que la temporización en una línea serie con transmisión síncrona está controlada por dos relojes (uno en el emisor y otro en el receptor) cada uno de los cuales tiene una variación de un minuto cada año. ¿Cuál es la longitud máxima de una secuencia de bits sin que ocurra ningún problema de sincronización? Supóngase que un bit será correcto si se muestrea dentro del 40% en torno a su instante central y que el emisor y el receptor se sincronizan al principio de cada trama. Obsérvese que la velocidad de transmisión no es un factor a tener en cuenta, ya que tanto el periodo de un bit como el error absoluto de la temporización decrecen proporcionalmente al aumentar la velocidad de transmisión.

6.7. Si se incluyera un bit de paridad en cada carácter, ¿cambiaría la probabilidad de recibir un mensaje correctamente?

6.8. ¿Cuál es el objetivo de usar aritmética módulo 2 en lugar de usar aritmética binaria al calcular la FCS?

6.9. Suponga una trama con dos caracteres de cuatro bits cada uno. Sea la probabilidad de error de bit (independiente para cada bit) igual a 10^{-3}.

a) ¿Cuál es la probabilidad de que la trama recibida contenga al menos un bit erróneo?

b) Ahora añádase un bit de paridad a cada carácter. ¿Cuál es la probabilidad?

6.10. Usando el polinomio CRC-CCITT, genere el código de CRC de 16 bits para un mensaje formado por un 1 seguido de quince 0.

a) Haga uso de una división.

b) Utilice el mecanismo de la Figura 6.6 consistente en un registro de desplazamiento.

6.11. Explique con palabras por qué la implementación de una CRC mediante un registro de desplazamiento generará una salida de todo ceros en el receptor si no hay errores en la transmisión. Demuéstrelo con un ejemplo.

6.12. Determine la CRC para $P = 110011$ y $M = 11100011$.

6.13. Se diseña un procedimiento CRC para generar una FCS de 4 bits para mensajes de 11 bits. El polinomio generador es $X^4 + X^3 + 1$.

a) Dibuje el circuito con un registro de desplazamiento que realizaría esta función (*véase* la Figura 6.6).

b) Codifique la secuencia de datos 10011011100 (siendo el bit de la izquierda el menos significativo) utilizando el polinomio generador y obtenga la palabra-código.

c) Ahora suponga que el 7.º bit (contando desde el menos significativo) es erróneo y muestre que el algoritmo detecta el error.

6.14. **a)** En un esquema de detección de errores que usa CRC, se elige $P(x) = x^4 + x + 1$. Codifique los bits 10010011011.

b) Suponga que el canal introduce un patrón de errores 100010000000000 (es decir, invierte el bit 1 y el 5) ¿Qué se recibirá? ¿Puede detectarse este error?

c) Repetir el punto b para el patrón de errores 100110000000000.

6.15. En algunas normas de comunicación se utiliza un procedimiento de CRC definido de la siguiente manera:

$$\frac{X^{16}M(X) + X^k L(X)}{P(X)} = Q + \frac{R(X)}{P(X)}$$

$$\text{FCS} = L(X) + R(X)$$

donde

$$L(X) = X^{15} + X^{14} + X^{13} + \cdots + X + 1$$

y es el número de bits a comprobar (campos de dirección, control e información).

a) Describa con palabras el funcionamiento de este procedimiento.

b) Explique los beneficios potenciales.

c) Muestre la implementación utilizando registros de desplazamiento para

$$P(X) = X^{16} + X^{12} + X^5 + 1$$

6.16. Calcule la distancia de Hamming de las siguientes palabras-código:

a) 00000, 10101, 01010

b) 000000, 010101, 101010, 110110

6.17. En la Sección 6.4 se estudian los códigos para la corrección de errores, los cuales toman sus decisiones basándose en la distancia de Hamming. Es decir, dado un código formado por s palabras-código equiprobables de longitud n, para cada secuencia recibida $\mathbf{v}$, el receptor selecciona la palabra-código $\mathbf{w}$ para la cual la distancia $d(\mathbf{w}, \mathbf{v})$ es mínima. Nos gustaría demostrar que este esquema es «ideal» en el sentido de que el receptor siempre selecciona la palabra-código para la cual $p(\mathbf{w}|\mathbf{v})$, la probabilidad de $\mathbf{w}$ dado $\mathbf{v}$, es máxima. Debido a que todas las palabras-código se suponen equiprobables, la palabra-código que maximiza $p(\mathbf{w}|\mathbf{v})$ es la misma que maximiza $p(\mathbf{v}|\mathbf{w})$.

a) Para que $\mathbf{w}$ se reciba como si fuera $\mathbf{v}$, tiene que haber exactamente $d(\mathbf{w}, \mathbf{v})$ errores en la transmisión y, además, estos errores deben darse en aquellos bits en los $\mathbf{w}$ y $\mathbf{v}$ discrepen. Sea β la probabilidad de que un bit determinado se transmita incorrectamente y n la longitud de la palabra-código. Obtenga una expresión para $p(\mathbf{w}|\mathbf{v})$ en función de β, $d(\mathbf{w}, \mathbf{v})$ y n. *Sugerencia:* el número de bits erróneos es $d(\mathbf{w}, \mathbf{v})$ y el número de bits correctos es $n - d(\mathbf{w}, \mathbf{v})$.

b) Ahora compárese $p(\mathbf{v}|\mathbf{w}_1)$ y $p(\mathbf{v}|\mathbf{w}_2)$ para dos palabras-código diferentes, $\mathbf{w}_1$ y $\mathbf{w}_2$, calculando $p(\mathbf{v}|\mathbf{w}_1)/p(\mathbf{v}|\mathbf{w}_2)$.

c) Suponga que $0 < \beta < 0{,}5$ y demuestre que $p(\mathbf{v}|\mathbf{w}_1) > p(\mathbf{v}|\mathbf{w}_2)$ si y solamente si $d(\mathbf{v}, \mathbf{w}_1) < d(\mathbf{v}, \mathbf{w}_2)$. Esto probaría que la palabra-código $\mathbf{w}$, que obtiene el mayor valor de $p(\mathbf{v}|\mathbf{w})$, es la palabra cuya distancia a $\mathbf{v}$ es mínima.

6.18. En la Sección 6.4 se afirma que para todo entero positivo t, si el código verifica que $d_{\text{mín}} \geqslant 2t + 1$, entonces el código puede corregir todos los errores de hasta t bits. Demuestre esta afirmación. *Sugerencia:* empiece observando que para que una palabra-código $\mathbf{w}$ se decodifique como $\mathbf{w}'$, la secuencia recibida debe ser al menos tan cercana a $\mathbf{w}'$ como a $\mathbf{w}$.

6.19. Dibuje un diagrama de tiempos en el que se indique el estado de todos los circuitos EIA-232 entre dos parejas de DTE-DCE durante el curso de una llamada en una red telefónica conmutada.

6.20. Explique el funcionamiento de cada una de las conexiones en la configuración módem nulo de la Figura 6.14.

6.21. ¿Qué circuitos deben estar lógicamente conectados para que el circuito de bucle remoto funcione correctamente en V.24/EIA-232?

CAPÍTULO 7

Protocolos de control del enlace de datos

7.1. Control de flujo
Control de flujo mediante parada y espera
Control de flujo mediante ventana deslizante

7.2. Control de errores
ARQ con parada y espera
ARQ con vuelta atrás N
ARQ con rechazo selectivo

7.3. Control del enlace de datos de alto nivel (HDLC)
Características básicas
Estructura de trama
Funcionamiento

7.4. Lectura recomendadas

7.5. Términos clave, cuestiones de repaso y problemas
Términos clave
Cuestiones de repaso
Problemas

Apéndice 7A. Análisis de prestaciones
Control de flujo mediante parada y espera
Control de flujo sin errores mediante ventana deslizante
ARQ

CUESTIONES BÁSICAS

- Las técnicas de sincronización y gestión de la interfaz resultan insuficientes para dar respuesta a la potencial aparición de errores en una transmisión y a la posible necesidad de regulación de la velocidad de datos por parte del receptor. Es necesario, por tanto, incluir en cada dispositivo de comunicación una capa de control que regule el flujo de información, además de detectar y controlar los errores. Esta capa se denomina **protocolo de control del enlace de datos**.
- **El control de flujo** permite al receptor regular el flujo de los datos enviados por el emisor, de manera que la memoria temporal del primero no se desborde.
- En un protocolo de control del enlace de datos, **el control de errores** se lleva a cabo mediante la retransmisión de las tramas dañadas que no hayan sido confirmadas o de aquellas para las que el otro extremo solicite su retransmisión.

Nuestro estudio se ha centrado hasta ahora en el *envío de señales sobre un enlace de transmisión*. Si se desea conseguir que la comunicación digital de datos sea efectiva, se precisa mucho más para controlar y gestionar el intercambio. En este capítulo centraremos nuestra atención en el *envío de datos sobre un enlace de comunicaciones*. Para llevar a cabo el control necesario se necesita una capa lógica adicional por encima de la interfaz física estudiada en el Capítulo 6; esta lógica se denomina **control del enlace de datos** o **protocolo de control del enlace de datos**. Cuando se usa un protocolo del enlace de datos, el medio de transmisión existente entre sistemas se denomina **enlace de datos**.

La necesidad del control del enlace de datos se evidencia a partir de los siguientes requisitos y objetivos para la comunicación efectiva de datos entre dos estaciones conectadas directamente:

- **Sincronización de trama:** los datos se envían en bloques denominados tramas, cuyo principio y fin deben ser identificables. Este aspecto se abordó brevemente cuando se estudiaron las tramas síncronas (*véase* Figura 6.2).
- **Control de flujo:** la estación emisora no debe enviar tramas a una velocidad superior a la que la estación receptora pueda absorberlas.
- **Control de errores:** se debe corregir cualquier error en los bits provocado por el sistema de transmisión.
- **Direccionamiento:** en una línea multipunto, como por ejemplo una red de área local (LAN), se debe identificar a las dos estaciones involucradas en una transmisión.
- **Datos y control sobre el mismo enlace:** por lo general, no se desea tener un canal de comunicaciones independiente para la información de control. En consecuencia, el receptor deberá ser capaz de diferenciar entre la información de control y los datos.
- **Gestión del enlace:** el inicio, mantenimiento y finalización de un intercambio de datos precisa un alto grado de coordinación y cooperación entre las estaciones. Se necesitan, pues, una serie de procedimientos para llevar a cabo la gestión de este intercambio.

Ninguno de los requisitos anteriores se cumple en las técnicas de gestión de la interfaz física estudiadas en el Capítulo 6. En este capítulo se verá que un protocolo que satisfaga todos los requisitos mencionados resulta bastante complejo. Comenzaremos considerando los dos mecanismos clave

que son parte del control del enlace de datos: el control de flujo y el control de errores. Después de estudiar los procedimientos básicos anteriores, se considerará el ejemplo de protocolo de control del enlace más significativo: HDLC (*High level Data Link Control*). Este protocolo es importante por dos razones: en primer lugar, porque es un estándar bastante utilizado; y segundo, porque HDLC ha servido como referencia para el desarrollo de la práctica totalidad del resto de protocolos de control del enlace importantes. Finalmente, en el apéndice de este capítulo se tratan algunas cuestiones relacionadas con el análisis de las prestaciones del control del enlace de datos.

7.1. CONTROL DE FLUJO

El control de flujo es una técnica utilizada para asegurar que una entidad de transmisión no sobrecargue a la entidad receptora con una excesiva cantidad de datos. Generalmente, la entidad receptora reserva una zona de memoria temporal para la transferencia. Cuando se reciben los datos, el receptor debe realizar cierta cantidad de procesamiento antes de pasar los datos al software de las capas superiores. En ausencia de procedimientos para el control de flujo, la memoria temporal del receptor se podría llenar y desbordarse mientras éste se encuentra procesando datos previos.

Comenzaremos estudiando el control de flujo en ausencia de errores. El modelo a usar se muestra en la Figura 7.1a, consistente en un diagrama donde el tiempo se representa sobre la vertical. Este diagrama es útil en cuanto que muestra las dependencias temporales y proporciona de forma adecuada la relación existente entre el emisor y el receptor. Cada flecha representa una única trama que transita por el enlace de datos establecido entre dos estaciones. Los datos se envían en base a una secuencia de tramas, en la que cada una de ellas contiene un campo de datos más

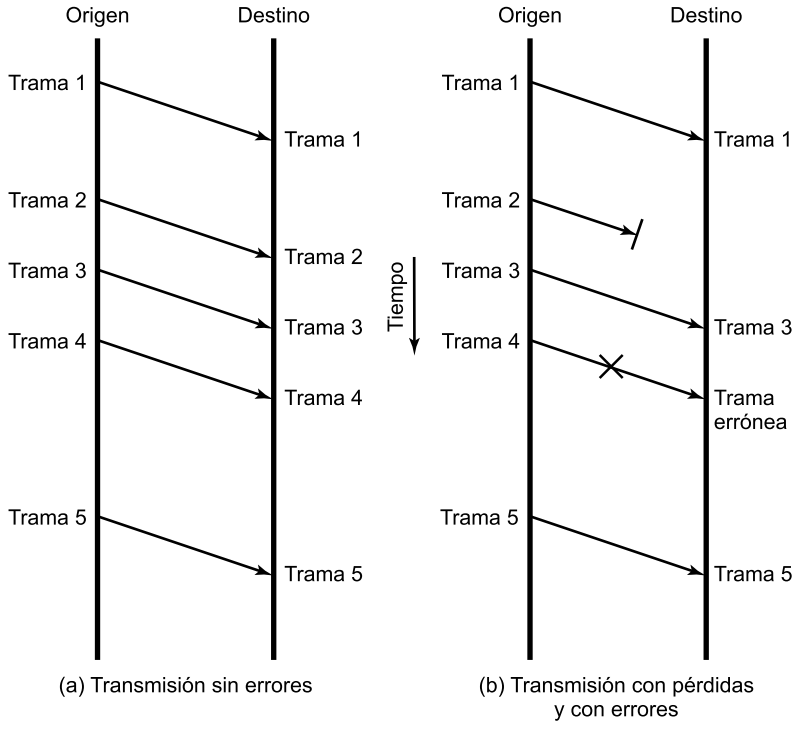


Figura 7.1. Modelo de transmisión de tramas.

información de control. Se define el tiempo de transmisión como el tiempo empleado por una estación para emitir todos los bits de una trama sobre el medio; este tiempo es proporcional a la longitud de la trama. Se define el tiempo de propagación como el tiempo empleado por un bit en atravesar el medio de transmisión desde el origen hasta el destino. Por ahora, supondremos que todas las tramas que se transmiten se reciben con éxito; ninguna trama se pierde y ninguna llega con errores. Es más, las tramas llegan en el mismo orden en que fueron transmitidas. No obstante, cada trama transmitida sufrirá un retardo arbitrario y variable antes de ser recibida[1].

CONTROL DE FLUJO MEDIANTE PARADA Y ESPERA

El procedimiento más sencillo para controlar el flujo, denominado control de flujo mediante parada y espera, funciona de la siguiente manera. Una entidad origen transmite una trama. Tras la recepción, la entidad destino indica su deseo de aceptar otra trama mediante el envío de una confirmación de la trama que acaba de recibir. El origen debe esperar a recibir la confirmación antes de proceder a la transmisión de la trama siguiente. De este modo, el destino puede parar el flujo de los datos sin más que retener las confirmaciones. Este procedimiento funciona adecuadamente y, de hecho, es difícil mejorar sus prestaciones cuando el mensaje se envía usando un número reducido de tramas de gran tamaño. No obstante, es frecuente que el origen segmente la información en bloques pequeños, transmitiendo los datos en varias tramas. Esto se hace así por las siguientes razones:

- El tamaño de la memoria temporal del receptor puede ser limitado.
- Cuanto más larga sea la transmisión es más probable que haya errores, precisándose en tal caso la retransmisión de la trama completa. Si se usan tramas más pequeñas, los errores se detectarán antes y, en consecuencia, se necesitará retransmitir una cantidad de datos menor.
- En un medio compartido, como por ejemplo una LAN, es frecuente que no se permita que una estación ocupe el medio durante un periodo de tiempo largo, evitándose así que las otras estaciones transmisoras sufran grandes retardos.

Si se usan varias tramas para un solo mensaje, puede resultar inadecuado el empleo del procedimiento de parada y espera. Esencialmente, el problema radica en que sólo puede haber una trama en tránsito en un instante de tiempo dado. Para explicar este hecho definamos la longitud de un enlace en bits como:

$$B = R \times \frac{d}{V}$$

donde

B = longitud del enlace en bits; es decir, el número de bits presentes en el enlace cuando una secuencia de ellos lo ocupa completamente.

R = velocidad del enlace, en bps.

d = longitud, o distancia, del enlace en metros.

V = velocidad de propagación, en m/s.

En aquellas situaciones en las que la longitud del enlace en bits es mayor que la longitud de la trama, aparecen ineficiencias importantes. Estos problemas se muestran en la Figura 7.2. En ella,

[1] En un enlace punto a punto directo, el retardo suele ser fijo en lugar de variable. Sin embargo, se puede utilizar un protocolo de control del enlace de datos en una conexión de red, como por ejemplo un circuito conmutado o una red ATM, en cuyo caso el retardo puede ser variable.

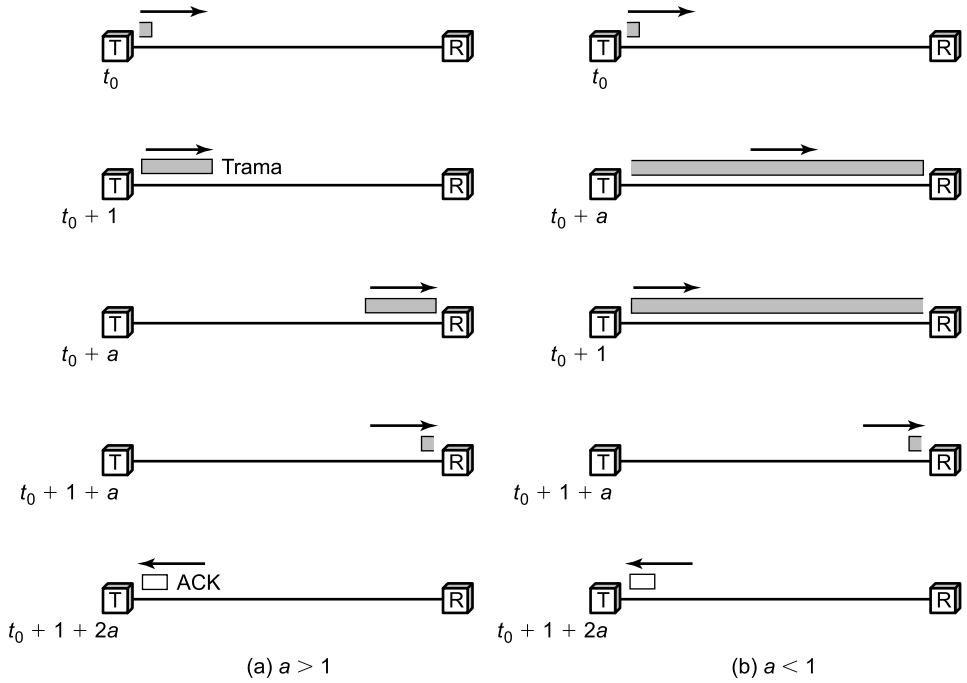


Figura 7.2. Utilización del enlace en parada y espera (tiempo de transmisión = 1; tiempo de propagación = a).

el tiempo de transmisión (tiempo que tarda una estación en transmitir una trama) se normaliza a la unidad y el retardo de propagación (tiempo que tarda un bit en ir desde el emisor hasta el receptor) se expresa como la variable a. Así, podemos expresar el parámetro a como

$$a = \frac{B}{L}$$

donde L es el número de bits en la trama (longitud de la trama en bits).

Cuando a es menor que 1, el tiempo de propagación es menor que el de transmisión. En este caso, la trama es lo suficientemente larga para que los primeros bits de la misma lleguen al destino antes de que el origen haya concluido la transmisión de dicha trama. Cuando a es mayor que 1, el tiempo de propagación es mayor que el de transmisión. En este caso, el emisor completa la transmisión de toda la trama antes que el primer bit de la misma llegue al receptor. Es decir, para velocidades de transmisión y/o distancias grandes es aconsejable la utilización de valores grandes de a. En el Apéndice 7.A se analizan las prestaciones del enlace de datos y el parámetro a.

Las dos partes de la Figura 7.2 (a y b) consisten en una secuencia de instantáneas del proceso de transmisión tomadas a lo largo del tiempo. En ambos casos, las cuatro primeras instantáneas muestran el proceso de la transmisión de una trama que contiene datos, correspondiendo el último esquema a la devolución de una trama de confirmación pequeña. Obsérvese que, para $a > 1$, la línea está siempre infrautilizada, e incluso para el caso $a < 1$, la línea se utiliza de forma ineficiente. Resumiendo, el procedimiento de control de flujo mediante parada y espera da lugar a una utilización ineficiente de la línea para el caso de velocidades de transmisión muy altas entre emisores y receptores que se encuentran separados a grandes distancias.

Ejemplo 7.1. Considérese un enlace de fibra óptica de 200 metros a 1 Gbps. La velocidad de propagación en la fibra óptica es, generalmente, del orden de 2×10^8 m/s. Haciendo uso de la Ecuación (7.1), $B = (10^9 \times 200)/(2 \times 10^8) = 1.000$. Supóngase la transmisión de una trama de 1.000 bytes, u 8.000 bits. Haciendo uso de la Ecuación (7.2), $a = (1.000/8.000) = 0{,}125$. Tomando como base la Figura 7.2b, considérese que la transmisión comienza en $t = 0$. Tras 1 μs (un tiempo normalizado de 0,125 intervalos de trama), el inicio de la trama (primer bit) ha llegado a R y los 1.000 primeros bits de la trama se encuentran ya sobre el enlace. En $t = 8$ μs, el final de la trama (último bit) acaba de ser emitido por T y los 1.000 últimos bits de la trama se encuentran sobre el enlace. En $t = 9$ μs, el bit final de la trama llega a R, el cual procederá a devolver una trama ACK. Si suponemos despreciable el tiempo de transmisión de la trama ACK (la cual es muy pequeña) y que ésta se envía inmediatamente, el ACK llega a T en $t = 10$ μs. Llegados a este punto, T puede comenzar a transmitir una nueva trama. El tiempo de transmisión real de la trama es 8 μs, pero el total de su transmisión y recepción del ACK es 10 μs.

Considérese ahora un enlace de 1 Mbps entre dos estaciones terrestres que se comunican vía satélite. Un satélite geoestacionario está situado a una altura aproximada de 36.000 km, por lo que $B = (10^6 \times 2 \times 36.000.000)/(3 \times 10^6) = 240.000$. Para una trama de 8.000 bits de longitud, $a = (240.000/8.000) = 30$. Tomando como base la Figura 7.2a, podemos seguir los mismos pasos que antes, resultando un tiempo igual a 240 ms para que el inicio de la trama se reciba y 8 ms adicionales para el resto de la trama. Por su parte, la trama ACK llega a T en $t = 488$ ms. El tiempo de transmisión real para la primera trama es de 8 ms, pero el total involucrado en su transmisión y en la recepción del ACK es 488 ms.

CONTROL DE FLUJO MEDIANTE VENTANA DESLIZANTE

El problema comentado con anterioridad radica básicamente en el hecho de que sólo puede haber en tránsito una trama a la vez. En todas aquellas situaciones en las que la longitud del enlace en bits sea mayor que la longitud de la trama ($a > 1$), aparecerán problemas graves de ineficiencia. Si se permite que transiten varias tramas al mismo tiempo sobre el enlace, la eficiencia mejorará significativamente.

Veamos cómo funcionaría este procedimiento para dos estaciones, A y B, conectadas mediante un enlace *full-duplex*. La estación B reserva memoria temporal suficiente para almacenar W tramas. Por tanto, B puede aceptar W tramas, permitiéndosele a A enviar este mismo número de tramas sin tener que esperar ninguna confirmación. Para saber qué tramas se han confirmado, cada una de ellas se etiqueta con un número de secuencia. B confirma una trama mediante el envío de una confirmación que incluye el número de secuencia de la siguiente trama que se espera recibir. Esta confirmación informa también, implícitamente, acerca de que B está preparado para recibir las W tramas siguientes, comenzando por la de número especificado. Este esquema se puede utilizar también para confirmar varias tramas simultáneamente. Por ejemplo, B podría recibir las tramas 2, 3 y 4, pero retener la confirmación hasta que llegase la trama 4. Al devolver una confirmación con número de secuencia 5, B confirma simultáneamente las tramas 2, 3 y 4. A mantiene una lista con los números de secuencia que se le permite transmitir y B mantiene una lista con los números de secuencia que está esperando recibir... Cada una de estas listas se puede considerar como una *ventana* de tramas, de ahí que este procedimiento se denomine **control de flujo mediante ventana deslizante** (*sliding-window flow control*).

Es necesario hacer algunos comentarios adicionales. Debido a que la numeración de las tramas ocupa un campo en las mismas, es evidente que dicha numeración tendrá un tamaño limitado. Por

ejemplo, si se considera un campo de 3 bits, los números de secuencia pueden variar entre 0 y 7. Por consiguiente, las tramas se numerarán módulo 8; es decir, después del número 7 vendrá el 0. En general, para un campo de k bits el rango de números de secuencia irá desde 0 hasta 2^{k-1}, numerándose las tramas módulo 2^k. Como se verá más adelante, el tamaño máximo de la ventana es 2^{k-1}.

Teniendo esto en cuenta, la Figura 7.3 muestra una forma útil de representar el procedimiento de ventana deslizante. En esta figura se consideran números de secuencia de 3 bits, por lo que las tramas se numerarán secuencialmente desde 0 a 7, utilizando los mismos números cíclicamente para las tramas sucesivas. El rectángulo sombreado indica las tramas que se pueden transmitir; en el ejemplo de la figura el emisor puede transmitir cinco tramas, comenzando por la 0. Cada vez que se envíe una trama, la ventana sombreada se cerrará, reduciendo su tamaño; cada vez que se reciba una confirmación, la ventana sombreada se abrirá. Las tramas comprendidas entre la barra vertical y la ventana sombreada han sido ya enviadas, pero aún no han sido confirmadas. Como se verá posteriormente, el emisor debe almacenar estas tramas en la memoria temporal por si hubiera que retransmitirlas.

Dada una longitud para los números de secuencia, el tamaño de la ventana real no necesita ser el máximo posible. Por ejemplo, si se usan números de secuencia de 3 bits, se podría configurar un tamaño para la ventana igual a 4 para las estaciones que utilicen el protocolo de ventana deslizante.

En la Figura 7.4 se muestra un ejemplo en el que se supone un campo de 3 bits para los números de secuencia y un tamaño máximo para la ventana igual a siete tramas. Inicialmente, A y B tienen las ventanas indicando que A puede transmitir siete tramas, comenzando con la 0 (F0). Tras transmitir tres tramas (F0, F1, F2) sin confirmación, A habrá cerrado su ventana hasta tener un

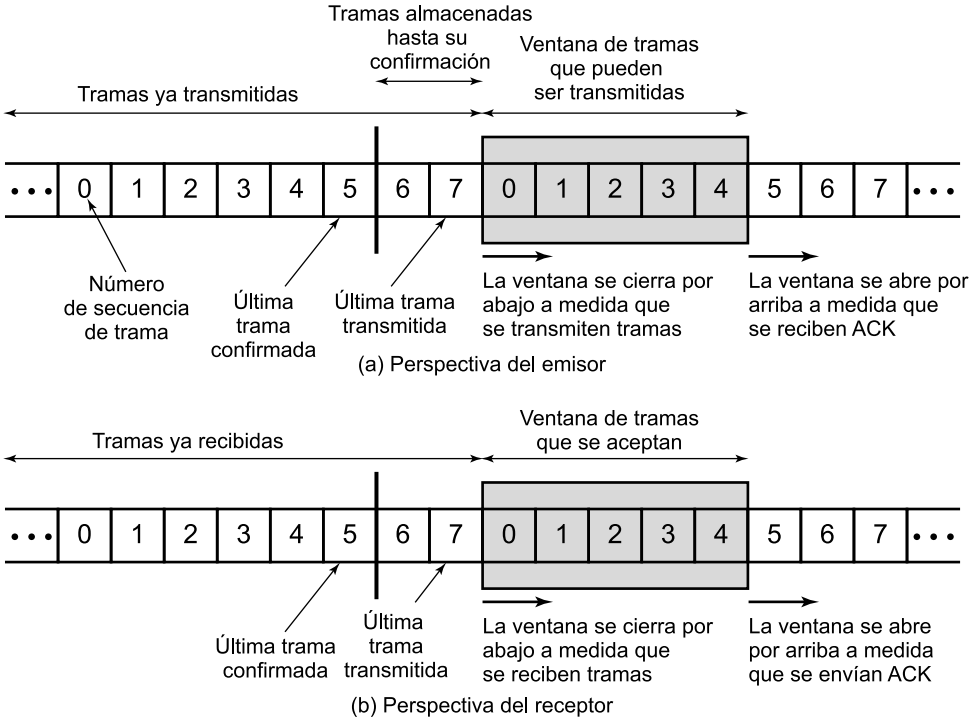

Tramas almacenadas hasta su confirmación
Ventana de tramas que pueden ser transmitidas
Tramas ya transmitidas
• • • 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 • • •
Número de secuencia de trama
Última trama confirmada
Última trama transmitida
La ventana se cierra por abajo a medida que se transmiten tramas
La ventana se abre por arriba a medida que se reciben ACK
(a) Perspectiva del emisor
Ventana de tramas que se aceptan
Tramas ya recibidas
• • • 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 • • •
Última trama confirmada
Última trama transmitida
La ventana se cierra por abajo a medida que se reciben tramas
La ventana se abre por arriba a medida que se envían ACK
(b) Perspectiva del receptor

Figura 7.3. Esquema de ventana deslizante.

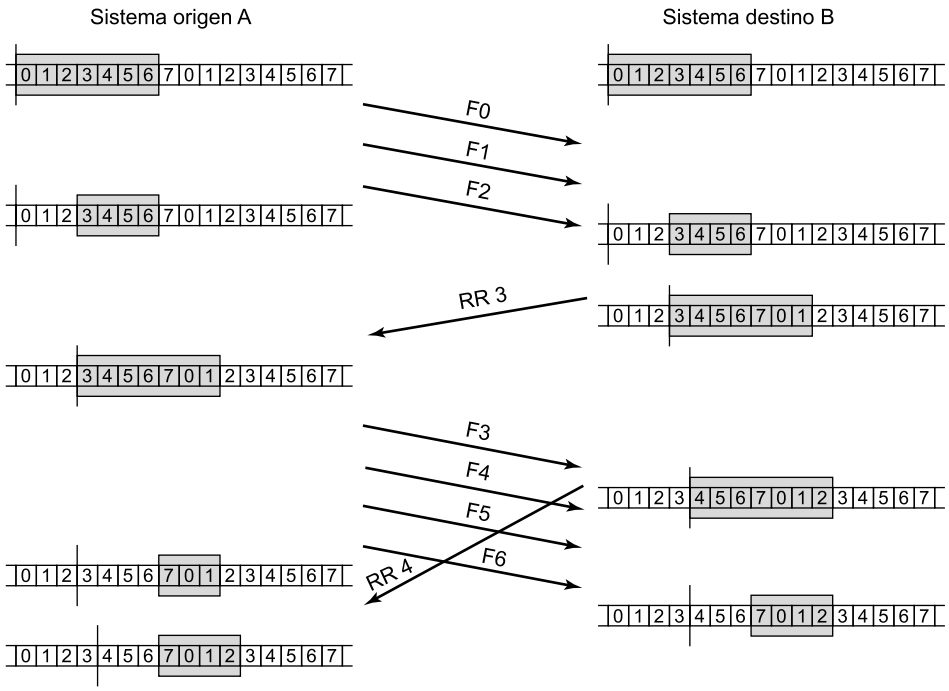


Figura 7.4. Ejemplo de transmisión mediante el protocolo de ventana deslizante.

tamaño de cuatro tramas, manteniendo una copia de las tres tramas transmitidas. La ventana indica que A puede transmitir cuatro tramas, comenzando por la número 3. B transmite entonces una trama RR (receptor preparado, *Receive Ready*) 3, lo que significa «he recibido todas las tramas hasta la número 2 y estoy preparado para recibir la número 3; de hecho, estoy preparado para recibir siete tramas, comenzando por la número 3». Tras ello, a la estación A se le permite transmitir siete tramas, comenzando por la trama 3; A también puede descartar las tramas almacenadas en la memoria temporal que acaban de ser confirmadas. A pasa a transmitir las tramas 3, 4, 5 y 6. B devuelve una RR 4, con la que confirma F3 y permite la posterior transmisión de la trama F4 y siguientes, hasta la F2. Cuando la trama RR llega a A, éste ya ha transmitido F4, F5 y F6, por lo que A sólo abre su ventana para permitir la transmisión de cuatro tramas a partir de la F7.

El mecanismo que se ha descrito proporciona un procedimiento para controlar el flujo: el receptor sólo acepta las siete tramas siguientes a la última que ha confirmado. La mayoría de los protocolos permiten también que una estación pueda interrumpir totalmente la transmisión de tramas desde el otro extremo mediante el envío de un mensaje RNR (receptor no preparado, *Receive Not Ready*), con el que se confirman las tramas anteriores pero se prohíbe la transmisión de tramas adicionales. Así, RNR 5 significa: «he recibido todas las tramas hasta la número 4 pero no acepto más». En algún momento posterior, la estación deberá transmitir una confirmación normal que «reabra» la ventana.

Hasta ahora hemos considerado la transmisión de tramas en una sola dirección. Si dos estaciones intercambian datos, cada una de ellas deberá mantener dos ventanas, una para transmitir y otra para recibir, y cada extremo deberá enviar hacia el otro tanto datos como confirmaciones. Para llevar a cabo esto de forma eficiente se utiliza un procedimiento denominado **incorporación de confirmación** (*piggybacking* en inglés). Cada **trama de datos** incluye un campo en el que se indica el número de secuencia de dicha trama más un campo que indica el número de secuencia que se

confirma. Por tanto, si una estación tiene para enviar una confirmación además de datos, lo hará conjuntamente utilizando una sola trama, ahorrando así capacidad del canal. Por supuesto, si una estación tiene que enviar una confirmación pero no tiene datos, se enviará una **trama de confirmación**, como por ejemplo una RR o una RNR. Si la estación tiene datos para enviar pero nada que confirmar, deberá repetir el último número de secuencia de confirmación enviado con anterioridad. Esto se debe a que en la trama de datos se prevé un campo para el número de confirmación y, por tanto, habrá que especificar algún valor en el mismo. Cuando una estación reciba una confirmación repetida, simplemente la ignorará.

El control de flujo mediante ventana deslizante es potencialmente mucho más eficiente que el control de flujo mediante un procedimiento de parada y espera. La razón se debe a que con un control de flujo mediante ventana deslizante, el enlace de transmisión se trata como si fuese una tubería que se puede rellenar con tramas en tránsito. Por el contrario, en el control de flujo mediante parada y espera sólo cabe una trama en la tubería. En el Apéndice 7.A se estudian las mejoras obtenidas en la eficiencia en términos cuantitativos.

Ejemplo 7.1. Considérese el empleo de un esquema de control de flujo mediante ventana deslizante para las dos configuraciones del Ejemplo 7.1. Como determinamos entonces, la recepción de una trama ACK correspondiente a la primera trama de datos conlleva 10 μs. Se tardan 8 μs en transmitir una trama de datos, por lo que el emisor puede emitir una trama y parte de otra hasta que se recibe el ACK de la primera. Así, un tamaño de ventana igual a 2 es adecuado para permitir al emisor transmitir tramas de forma continua, o a una velocidad de una trama cada 8 μs. Con el esquema de parada y espera sólo es posible una velocidad de una trama cada 10 μs.

En la configuración de satélite transcurren 488 ms hasta que se recibe el ACK correspondiente a la primera trama de datos. Se tardan 8 ms en transmitir una trama, por lo que el emisor puede transmitir 61 tramas hasta que se recibe el ACK de la primera. Con un tamaño de ventana igual a 6 bits o más, el emisor puede transmitir continuamente, o a una velocidad de una trama cada 8 ms. Si el tamaño de ventana fuese 7, mediante el empleo de un campo de ventana de 3 bits, el emisor sólo puede enviar 7 tramas, tras lo cual debe esperar un ACK antes de poder continuar transmitiendo. En este caso, el emisor puede transmitir a una velocidad de 7 tramas cada 488 ms, o en torno a una trama cada 70 ms. En cambio, mediante parada y espera sólo es posible una velocidad de una trama cada 488 ms.

7.2. CONTROL DE ERRORES

El control de errores hace referencia a los mecanismos necesarios para la detección y la corrección de errores que aparecen en una transmisión de tramas. En la Figura 7.1b se muestra el caso típico que se va a considerar como modelo. Como se ha considerado hasta ahora, los datos se envían en base a una secuencia de tramas, las cuales se reciben en el mismo orden en que fueron enviadas y cada una de ellas, con carácter previo a su recepción, sufre un retardo arbitrario y posiblemente variable. Se contemplan dos tipos de errores potenciales:

- **Tramas perdidas:** se produce cuando una trama enviada no llega al otro extremo. Así, por ejemplo, una ráfaga de ruido puede dañar una trama de manera que el receptor no se percate siquiera de su transmisión.

- **Tramas dañadas:** ocurre cuando una trama se recibe con algunos bits erróneos (modificados durante la transmisión).

Las técnicas más usuales para el control de errores se basan en algunas o todas las siguientes aproximaciones:

- **Detección de errores:** discutida en el Capítulo 6.
- **Confirmaciones positivas:** el destino devuelve una confirmación positiva por cada trama recibida con éxito, libre de errores.
- **Retransmisión tras la expiración de un temporizador:** la fuente retransmite las tramas que no se han confirmado tras un periodo de tiempo predeterminado.
- **Confirmación negativa y retransmisión:** el destino devuelve una confirmación negativa para aquellas tramas en las que se detecta la ocurrencia de errores. El origen retransmitirá de nuevo dichas tramas.

Estos mecanismos se denominan genéricamente **solicitud de repetición automática** (ARQ, *Automatic Repeat reQuest*); el objetivo de un esquema ARQ es convertir un enlace de datos no fiable en fiable. Hay tres variantes ARQ estandarizadas:

ARQ con parada y espera.

ARQ con vuelta atrás N.

ARQ con rechazo selectivo.

Todos estos procedimientos se basan en el empleo de las técnicas de control de flujo presentadas en la Sección 7.1. Estudiemos cada una de ellas.

ARQ CON PARADA Y ESPERA

El esquema ARQ con parada y espera se basa en la técnica para el control de flujo mediante parada y espera estudiada con anterioridad. La estación origen transmite una única trama y debe esperar la recepción de una confirmación (ACK). No se podrá enviar ninguna otra trama hasta que la respuesta de la estación destino llegue al emisor.

Pueden ocurrir dos tipos de error. El primero consiste en que la trama que llega al destino puede estar dañada. El receptor detecta este hecho mediante la utilización de técnicas de detección de errores y, simplemente, descartará la trama. Para dar respuesta a esta situación, la estación fuente utiliza un temporizador. De este modo, tras el envío de una trama, la estación espera la recepción de una confirmación; si no se recibe ninguna confirmación antes de que el temporizador expire, se procederá a reenviar la misma trama. Obsérvese que este método exige que el emisor conserve una copia de la trama transmitida hasta que se reciba la confirmación correspondiente.

El segundo tipo de error se refiere a una confirmación deteriorada. Considérese la siguiente situación. Una estación A envía una trama, que se recibe correctamente en una estación B, la cual responde con una confirmación (ACK). La trama ACK se deteriora en el camino, de modo que no es identificable por A, por lo que se producirá una expiración del temporizador y se reenviará la misma trama de datos. Esta trama duplicada llega y se acepta por B. Así pues, B ha aceptado dos copias de la misma trama como si fueran distintas. Para evitar este problema, las tramas se pueden etiquetar de forma alternada con 0 o 1, siendo las confirmaciones positivas de la forma ACK0 y ACK1. Para mantener las convenciones adoptadas en el procedimiento de ventana deslizante, una trama ACK0 confirma la recepción de la trama numerada como 1 e indica que el receptor está preparado para aceptar la trama numerada como 0.

En la Figura 7.5 se muestra un ejemplo acerca de la utilización del esquema ARQ con parada y espera; en ella se ilustra la transmisión de una secuencia de tramas desde un origen A a un destino B. La figura muestra los dos tipos de error que se han comentado previamente. La tercera trama transmitida por A se daña o se pierde, por lo que B no devuelve ninguna trama ACK. En A se produce la expiración del temporizador y se retransmite la trama. Posteriormente, A transmite una trama etiquetada con 1 pero se pierde su correspondiente ACK0. El temporizador en A expira y se retransmite la trama. Cuando B recibe dos tramas consecutivas con la misma etiqueta, descarta la segunda pero devuelve una trama ACK0 para cada una de ellas.

La principal ventaja del esquema ARQ con parada y espera es su sencillez. Su desventaja más importante se discutió en la Sección 7.1, y no es otra que el procedimiento parada y espera es ineficiente. Para conseguir una utilización más eficiente de la línea se puede hacer uso de las técnicas de control de flujo mediante ventana deslizante, a las cuales se les suele referir como *ARQ continua*.

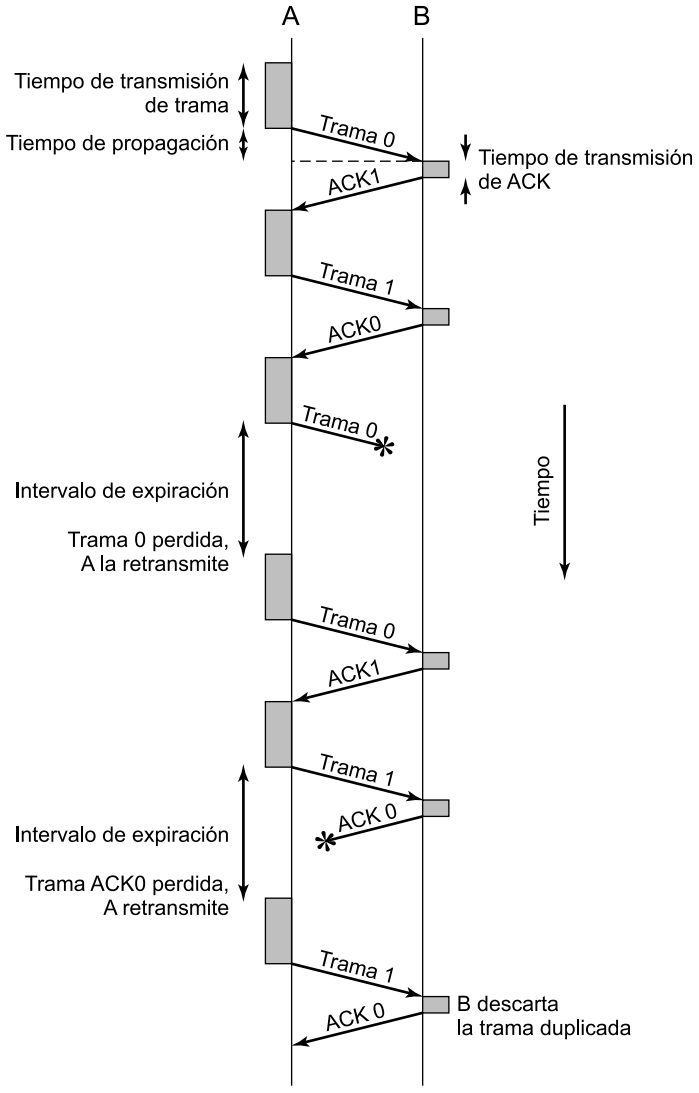


Figura 7.5. ARQ con parada y espera.

ARQ CON VUELTA ATRÁS N

La técnica de control de errores basada en el control de flujo mediante ventana deslizante más frecuentemente usada se denomina ARQ con vuelta atrás N. En esta técnica, una estación puede enviar una serie de tramas numeradas secuencialmente módulo algún valor máximo dado. Al utilizar la técnica de control de flujo mediante ventana deslizante, el número de tramas pendientes de confirmar se determina mediante el tamaño de la ventana. Mientras no se produzcan errores, el destino confirmará las tramas recibidas como es habitual (mediante una trama RR o mediante la técnica de incorporación de confirmación, *piggybacking*). Si la estación destino detecta un error en una trama, puede llevar a cabo el envío de una confirmación negativa (REJ, REJect) para dicha trama como sigue. La estación destino descartará esa trama y todas las que se reciban con posterioridad hasta que dicha trama errónea llegue correctamente. Así, cuando la estación origen reciba un REJ, deberá retransmitir la trama errónea además de todas las posteriores que hayan sido transmitidas tras ella.

Considérese que una estación A envía tramas a una estación B. Después de cada transmisión, A inicia un temporizador para la confirmación de la trama que se acaba de enviar. Supóngase que B ha recibido la trama $(i - 1)$ sin errores y que A acaba de enviar la trama i. La técnica vuelta atrás N tiene en cuenta las siguientes contingencias:

1. **Trama deteriorada.** Si la trama recibida es no válida (es decir, B detecta un error en ella o la trama está tan dañada que B ni siquiera detecta su recepción), B descartará dicha trama sin más. Llegados a este punto se plantean dos posibilidades:

   a) A envía la trama $(i + 1)$ dentro de un periodo de tiempo razonable. B recibe la trama $(i + 1)$ fuera de orden y envía una REJ i. A debe retransmitir la trama i y todas las posteriores.

   b) A no envía tramas adicionales en un breve espacio de tiempo. B no recibe nada, por lo que ni devuelve una trama RR ni una REJ. Cuando el temporizador de A expira, esta estación transmite una trama RR que incluye un bit denominado P, que estará puesto a 1. B interpreta la trama RR con el bit P igual a 1 como si fuera una orden que debe ser confirmada mediante el envío de una trama RR para indicar la siguiente trama que se espera recibir, la i. Cuando A recibe la trama RR, retransmite la trama i. Esta retransmisión por parte de A puede realizarse también ante la expiración de su temporizador.

2. **Trama RR deteriorada.** Existen dos casos posibles:

   a) B recibe la trama i y envía una RR $(i + 1)$, que sufre un error en el camino. Dado que las confirmaciones son acumulativas (por ejemplo, RR 6 significa que se confirman todas las tramas hasta la 5), puede ocurrir que A reciba después una RR correspondiente a una trama posterior y que llegue antes de que el temporizador asociado a la trama i expire.

   b) Si el temporizador de A expira, dicha estación transmite una orden RR, como en el caso 1.b. A inicia otro temporizador, denominado temporizador del bit P. Si B no responde a la orden RR, o si la respuesta se deteriora a lo largo de su transmisión, entonces el temporizador del bit P en A expirará. A lo intentará de nuevo enviando otra orden RR, reiniciando el temporizador del bit P. Este procedimiento se repite una serie de veces. Si A no recibe la confirmación tras un número máximo de intentos, comenzará un procedimiento de reinicio.

3. **Trama REJ deteriorada.** La pérdida de una trama REJ es equivalente al caso 1b.

La Figura 7.6a es un ejemplo del flujo de tramas para un esquema ARQ con vuelta atrás N. Debido al retardo de propagación en la línea, mientras que la confirmación (positiva o negativa) vuelve a la estación emisora, se habrá enviado, al menos, una trama adicional tras la primera que está siendo confirmada. En este ejemplo se deteriora la trama 4. Las tramas 5 y 6 se reciben fuera de orden y son descartadas por B. Cuando llega la trama 5, B envía inmediatamente una trama REJ 4. Al recibirse esta trama en el emisor, éste debe retransmitir no sólo la 4, sino también la 5 y la 6. Obsérvese que el emisor debe conservar una copia de todas las tramas que haya enviado y que no estén confirmadas.

En la Sección 7.1 se mencionó que si se dispone de un campo de k bits para los números de secuencia, lo que permitiría un rango para éstos igual a 2^k, el tamaño máximo de la ventana estará

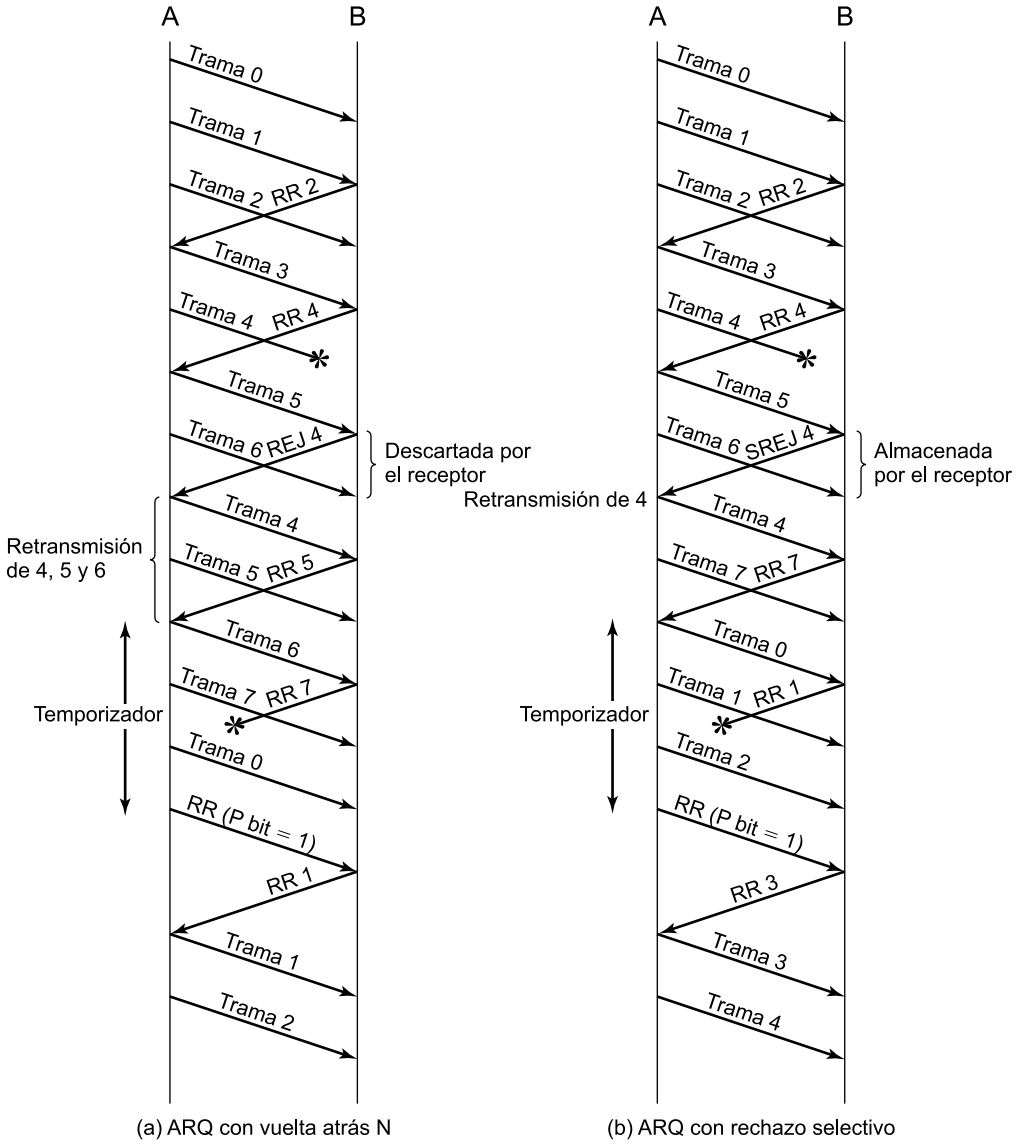


Figura 7.6. Protocolos ARQ mediante ventana deslizante.

limitado a 2^{k-1}. Esto se debe a la interacción entre los procedimientos para el control de errores y las confirmaciones. Téngase en cuenta que si los datos se están transmitiendo en ambos sentidos, la estación B debe enviar las confirmaciones correspondientes a las tramas enviadas por A dentro de sus propias tramas de datos mediante la técnica de incorporación de confirmaciones, incluso en el caso de que dichas confirmaciones hayan sido generadas ya con anterioridad. Como se ha mencionado, esto es debido a que B debe especificar algún valor en el campo previsto para las confirmaciones dentro de sus tramas de datos. A modo de ejemplo, supóngase que se utilizan números de secuencia de 3 bits (es decir, 8 números de secuencia). Supóngase que una estación envía la trama 0 y recibe de vuelta una RR 1; posteriormente envía las tramas 1, 2, 3, 4, 5, 6, 7, 0 y recibe otra RR 1. Esto podría significar que las 8 tramas se recibieron correctamente y que la RR 1 es una confirmación acumulativa. También podría interpretarse como que las 8 tramas se han deteriorado, o incluso perdido en el camino, y que la estación receptora está repitiendo la RR 1 anterior. Esta posible ambigüedad se evita si el tamaño máximo de la ventana se fija a 7 (es decir, $2^3 - 1$).

ARQ CON RECHAZO SELECTIVO

En el esquema ARQ con rechazo selectivo, las únicas tramas que se retransmiten son aquellas para las que se recibe una confirmación negativa, denominada SREJ (*Selective REJect*) ahora, o aquellas para las que el temporizador correspondiente expira. En la Figura 7.6b se muestra este esquema. Cuando la trama 5 se recibe fuera de orden, B envía una SREJ 4, indicando que la trama 4 no se ha recibido. Sin embargo, B sigue aceptando tramas y las almacena en la memoria temporal hasta que se reciba correctamente la trama 4. Llegados a este punto, B podrá proporcionar al software de las capas superiores las tramas en el orden correcto.

El procedimiento de rechazo selectivo puede parecer más eficiente que el de vuelta atrás N, puesto que minimiza el número de retransmisiones. Por otra parte, el receptor debe mantener una zona de memoria temporal lo suficientemente grande para almacenar las tramas recibidas tras el envío de una SREJ hasta que la trama errónea se retransmita; además, debe tener lógica adicional para reinsertar la trama reenviada en la posición correspondiente. Del mismo modo, el transmisor necesita también una lógica más compleja para poder enviar tramas fuera de orden. Debido a estas complicaciones, el esquema ARQ con rechazo selectivo se utiliza mucho menos que el ARQ con vuelta atrás N, aunque suele emplearse en enlaces satélite debido al elevado retardo de propagación involucrado.

La limitación en el tamaño máximo de la ventana es más restrictiva en el caso del esquema de rechazo selectivo que en el de vuelta atrás N. Considérese el caso de un procedimiento de rechazo selectivo que utiliza 3 bits para los números de secuencia. Permítase un tamaño de ventana igual a 7 y ténganse en cuenta las siguientes consideraciones [TANE03]:

1. La estación A envía las tramas desde la 0 hasta la 6 a la estación B.
2. La estación B recibe las siete tramas y las confirma acumulativamente mediante el envío de una trama RR 7.
3. Debido a una ráfaga de ruido, la trama RR 7 se pierde.
4. El temporizador de A expira y se retransmite la trama 0.
5. B ha desplazado su ventana de recepción indicando que acepta las tramas 7, 0, 1, 2, 3, 4 y 5. Al recibir la trama 0, supone que la 7 se ha perdido y que se trata de una trama 0 diferente, por lo que la acepta.

El problema aparecido en la casuística anterior se debe al solapamiento entre las ventanas de emisión y de recepción. Para evitar este problema, el tamaño máximo de la ventana no debería ser mayor que la mitad del rango de los números de secuencia. Así, en el escenario anterior se evitarían las ambigüedades si se permitiera que sólo estuvieran pendientes de confirmación 4 tramas. En general, para un campo de números de secuencia de k bits, es decir, para un rango igual a 2^k, el tamaño máximo de la ventana se limita a 2^{k-1}.

7.3. CONTROL DEL ENLACE DE DATOS DE ALTO NIVEL (HDLC)

El protocolo de control del enlace de datos más importante es HDLC (*High-level Data Link Control*, ISO 3009, ISO 4335). No sólo porque es ampliamente utilizado, sino también porque es la base de otros importantes protocolos de control del enlace, en los que se usan los mismos o similares formatos y los mismos procedimientos que los empleados en HDLC.

CARACTERÍSTICAS BÁSICAS

Para satisfacer las demandas de diversas aplicaciones, HDLC define tres tipos de estaciones, dos configuraciones del enlace y tres modos de operación para la transferencia de los datos. Los tres tipos de estaciones son:

- **Estación primaria:** es la responsable de controlar el funcionamiento del enlace. Las tramas generadas por la estación primaria se denominan órdenes.
- **Estación secundaria**: funciona bajo el control de la estación primaria. Las tramas generadas por la estación secundaria se denominan respuestas. La primaria establece un enlace lógico independiente con cada una de las secundarias presentes en la línea.
- **Estación combinada:** combina las características de las primarias y de las secundarias, pudiendo generar tanto órdenes como respuestas.

Las dos posibles configuraciones del enlace son:

- **Configuración no balanceada:** está formada por una estación primaria y una o más secundarias. Permite tanto transmisión *full-duplex* como *half-duplex*.
- **Configuración balanceada:** consiste en dos estaciones combinadas. Permite igualmente transmisión *full-duplex* y *half-duplex*.

Los tres modos de transferencia de datos son:

- **Modo de respuesta normal** (NRM, *Normal Response Mode*): se utiliza en la configuración no balanceada. La estación primaria puede iniciar la transferencia de datos hacia la secundaria, pero la secundaria sólo puede transmitir datos en base a respuestas a las órdenes emitidas por la primaria.
- **Modo balanceado asíncrono** (ABM, *Asynchronous Balanced Mode*): se utiliza en la configuración balanceada. En este modo, cualquier estación combinada puede iniciar la transmisión sin necesidad de recibir permiso por parte de la otra estación combinada.
- **Modo de respuesta asíncrono** (ARM, *Asynchronous Response Mode*): se utiliza en la configuración no balanceada. La estación secundaria puede iniciar la transmisión sin tener permiso explícito de la primaria. La estación primaria sigue teniendo la responsabilidad del

funcionamiento de la línea, incluyendo la iniciación, la recuperación de errores y la desconexión lógica.

El modo NRM se usa en líneas que disponen de múltiples conexiones, en las que se conectan varios terminales a un computador central; el computador sondea cada una de las entradas correspondientes a los distintos terminales. NRM también se usa a veces en enlaces punto a punto, principalmente si el enlace conecta un terminal u otros periféricos a un computador. ABM es el más utilizado de los tres modos; puesto que en ABM no se precisa realizar sondeos, la utilización de enlaces punto a punto *full-duplex* resulta más eficiente con este modo. ARM se utiliza en contadas ocasiones, pudiendo usarse en ciertas situaciones particulares en las que la estación secundaria necesita iniciar la transmisión.

ESTRUCTURA DE TRAMA

HDLC emplea transmisión síncrona. Todos los intercambios se realizan en base a tramas, siendo suficiente un único formato de trama para todos los tipos de intercambios de datos e información de control.

En la Figura 7.7 se muestra la estructura de la trama HDLC. Los campos de delimitación, de dirección y de control, que preceden al campo de información, se denominan **cabecera**. Los campos FCS y de delimitación, que están a continuación del campo de datos, se denominan **cola**.

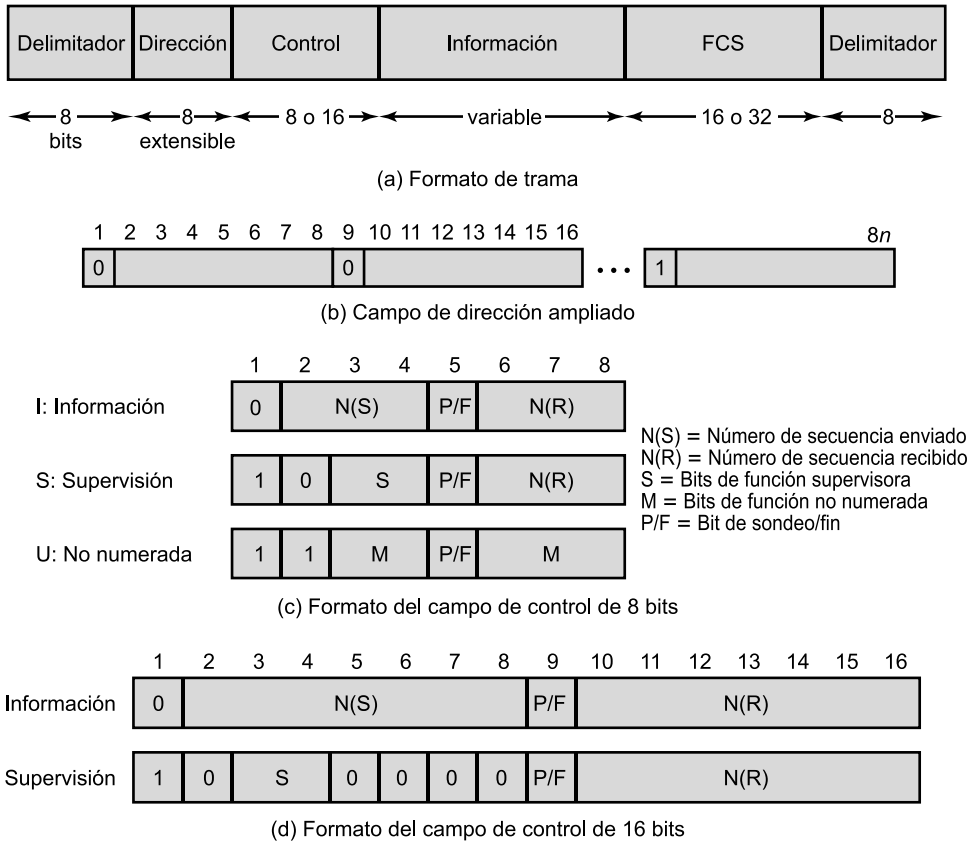

Delimitador
Dirección
Control
Información
FCS
Delimitador
8 bits
8 extensible
8 o 16
variable
16 o 32
8
(a) Formato de trama
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
8n
0
0
1
(b) Campo de dirección ampliado
1 2 3 4 5 6 7 8
I: Información
0 N(S) P/F N(R)
S: Supervisión
1 0 S P/F N(R)
U: No numerada
1 1 M P/F M
N(S) = Número de secuencia enviado
N(R) = Número de secuencia recibido
S = Bits de función supervisora
M = Bits de función no numerada
P/F = Bit de sondeo/fin
(c) Formato del campo de control de 8 bits
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Información
0 N(S) P/F N(R)
Supervisión
1 0 S 0 0 0 0 P/F N(R)
(d) Formato del campo de control de 16 bits

Figura 7.7. Estructura de la trama HDLC.

Campos de delimitación

Los campos de delimitación están localizados en los dos extremos de la trama y ambos corresponden al patrón de bits 01111110. Se puede usar un único delimitador como final de trama y comienzo de la siguiente simultáneamente. A ambos lados de la interfaz usuario-red, los receptores estarán continuamente intentando detectar la secuencia de delimitación para sincronizarse con el comienzo de la trama. Mientras se está recibiendo una trama, la estación sigue intentando detectar esa misma secuencia para determinar el final de la trama. Debido a que el protocolo permite cualquier combinación de bits (es decir, no se impone restricción alguna en el contenido de los campos), no hay garantía de que la combinación 01111110 no aparezca en algún lugar dentro de la trama, destruyendo de este modo la sincronización de las mismas. Para evitar este problema, se utiliza un procedimiento denominado *inserción de bits*. En la transmisión de los bits existentes entre los delimitadores de comienzo y de fin, el emisor insertará un 0 extra siempre que se encuentre con la aparición de cinco 1 consecutivos. El receptor, tras la detección del delimitador de comienzo, monitorizará la cadena de bits recibida de tal manera que cuando aparezca una combinación de cinco 1 seguidos, el sexto bit se analiza como sigue. Si dicho bit es 0, se eliminará sin más. Si el sexto bit es un 1 y el séptimo es un 0, la combinación se considera como un delimitador. Si los bits sexto y séptimo son ambos igual a 1, se interpreta como una indicación de cierre generada por el emisor.

El empleo del procedimiento de inserción de bits permite que en el campo de datos aparezca cualquier combinación arbitraria de bits. Esta propiedad se denomina **transparencia en los datos**.

En la Figura 7.8 se muestra un ejemplo de inserción de bits. Obsérvese que el 0 extra no es estrictamente necesario para los dos primeros casos, pero se necesita para el buen funcionamiento

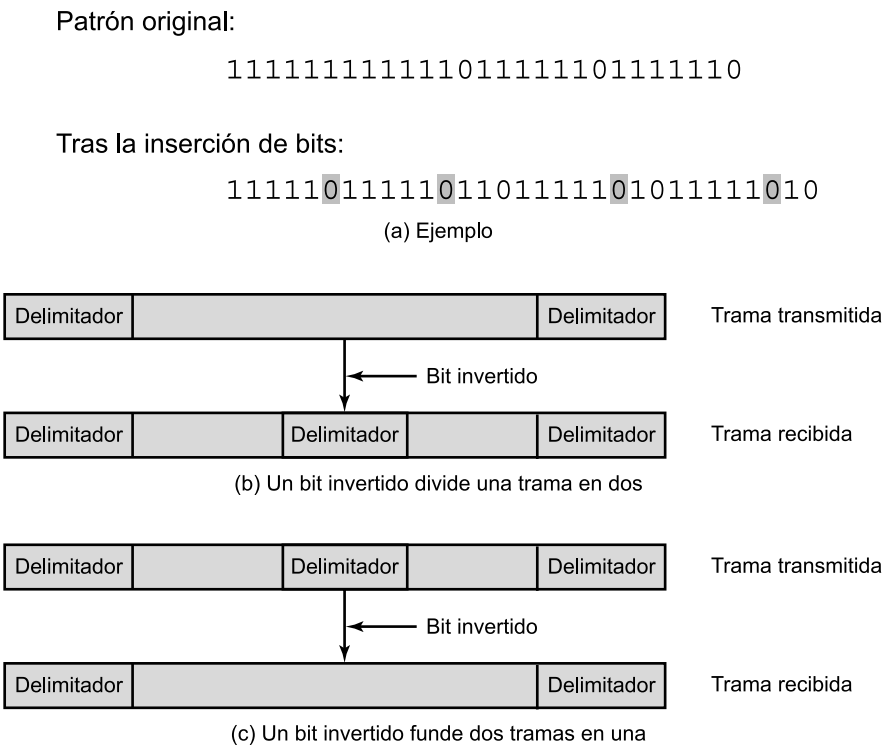


Figura 7.8. Inserción de bits.

del algoritmo. En esta figura también se muestran situaciones no deseadas que dan lugar a errores en la delimitación al considerar la inserción de bits. Cuando se usa un solo delimitador para el final y el comienzo, un simple error en un bit causaría que las dos tramas se fundieran en una. Del mismo modo, la aparición de un error en un solo bit dentro de la trama podría partir ésta en dos.

Campo de dirección

El campo de dirección identifica la estación secundaria que ha transmitido o va a recibir la trama. Este campo no se necesita en enlaces punto a punto, aunque se incluye siempre por cuestiones de uniformidad. El campo de dirección consta normalmente de 8 bits, si bien, tras una negociación previa, se puede utilizar un formato ampliado en el que la dirección es múltiplo de siete bits. El bit menos significativo de cada octeto será 1 o 0 en función de si es o no, respectivamente, el último octeto del campo de dirección. Los siete bits restantes de cada octeto constituyen la dirección propiamente dicha. Un octeto de la forma 11111111 se interpreta como una dirección que representa a todas las estaciones, tanto en el formato básico como en el ampliado. Este tipo de direccionamiento se utiliza cuando la estación primaria quiere enviar una trama a todas las secundarias.

Campo de control

En HDLC se definen tres tipos de tramas, cada una de ellas con un formato diferente para el campo de control. Las **tramas de información** (tramas-I) transportan los datos generados por el usuario (esto es, por la lógica situada en la capa superior, usuaria de HDLC). Además, en las tramas de información se incluye información para el control ARQ de errores y de flujo. Las **tramas de supervisión** (tramas-S) proporcionan el mecanismo ARQ cuando no se usa la incorporación de las confirmaciones en las tramas de información (*piggybacking*). Las **tramas no numeradas** (tramas-U, del inglés *unnumbered*) proporcionan funciones complementarias para controlar el enlace. El primero o los dos primeros bits del campo de control se utilizan para identificar el tipo de trama. Los bits restantes se organizan en subcampos como se indica en las Figuras 7.7c y d. Su utilización se explicará posteriormente en este mismo capítulo al estudiar el funcionamiento de HDLC.

Todos los formatos posibles del campo de control contienen el bit sondeo/fin (P/F, *poll/final*), cuya utilización es dependiente del contexto. Normalmente, en las tramas de órdenes se denomina bit P y se fija a valor 1 para solicitar (sondear) una trama de respuesta a la entidad HDLC par. En las tramas de respuesta, este bit se denomina F y se fija a valor 1 para identificar la trama de respuesta devuelta tras la recepción de una orden.

Obsérvese que el campo de control básico en las tramas-S y en las tramas-I utiliza números de secuencia de 3 bits. Mediante una orden que fije el modo adecuado, en estas tramas se puede hacer uso de un campo de control ampliado en el que los números de secuencia sean de 7 bits. Las tramas-U tienen siempre un campo de control de 8 bits.

Campo de información

El campo de información sólo está presente en las tramas-I y en algunas tramas-U. Este campo puede contener cualquier secuencia de bits, con la única restricción de que el número de bits sea igual a un múltiplo entero de octetos. La longitud del campo de información es variable y siempre será menor que un valor máximo predefinido.

Campo de secuencia de comprobación de trama

La secuencia de comprobación de trama (FCS, *Frame Check Sequence*) es un código para la detección de errores calculado a partir de los bits de la trama, excluyendo los delimitadores. El código que se usa normalmente es el CRC-CCITT de 16 bits definido en la Sección 7.2. También se puede utilizar un campo FCS de 32 bits, que haga uso del polinomio CRC-32, si así lo aconseja la longitud de la trama o las características de la línea.

FUNCIONAMIENTO

El funcionamiento de HDLC consiste en el intercambio de tramas-I, tramas-S y tramas-U entre dos estaciones. En la Tabla 7.1 se definen las órdenes y respuestas posibles para los distintos tipos de tramas. Estos tres tipos de tramas se explicarán a través de la descripción del funcionamiento de HDLC.

Tabla 7.1. Órdenes y respuestas HDLC.

Nombre	Órdenes/ respuesta	Descripción
Información (I)	C/R	Intercambio de datos de usuario
Supervisión (S)		
Receptor preparado (RR)	C/R	Confirmación positiva; preparado para recibir tramas I
Receptor no preparado (RNR)	C/R	Confirmación positiva; no preparado para recibir
Rechazo (REJ)	C/R	Confirmación negativa; vuelta atrás N
Rechazo selectivo (SREJ)	C/R	Confirmación negativa; rechazo selectivo
No numerada (N)		
Establecimiento de modo de respuesta normal/ampliado (SNRM/SNRME)	C	Establecimiento de modo, ampliado = números de secuencia de 7 bits
Establecimiento de modo de respuesta asíncrono normal ampliado (SARM/SARME)	C	Establecimiento de modo, ampliado = números de secuencia de 7 bits
Establecimiento de modo asíncrono balanceado normal/ampliado (SABM/SABME)	C	Establecimiento de modo, ampliado = números de secuencia de 7 bits
Establecimiento de modo inicialización (SIM)	C	Inicialización de las funciones de control del enlace en las estaciones especificadas en la dirección
Desconexión (DISC)	C	Finalización de la conexión lógica del enlace
Confirmación no numerada (UA)	R	Aceptación de confirmación de una de las órdenes de establecimiento de modo
Modo desconectado (DM)	R	La estación que responde se encuentra en el modo desconectado
Solicitud de desconexión (RD)	R	Solicitud de una orden DISC
Solicitud de modo de inicialización (RIM)	R	Se necesita inicializar; solicitud de la orden SIM
Información no numerada (UI)	C/R	Usada para intercambiar información de control
Sondeo no numerado (UP)	C	Usada para solicitar información de control
Reset (RSET)	C	Usada para recuperación, reinicia N(R) y N(S)
Identificación de intercambio (XID)	C/R	Usada para solitícar/informar el estado
Test (TEST)	C/R	Intercambio de campos de información idénticos para test
Rechazo de trama (FRMR)	R	Informa de la recepción de una trama inaceptable

El funcionamiento de HDLC implica tres fases. En primer lugar, uno de los dos extremos inicia el enlace de datos, de manera que las tramas se puedan intercambiar de una forma ordenada. Durante esta fase se acuerdan las opciones que se usarán en el intercambio posterior. Tras la iniciación, los dos extremos intercambian datos de usuario e información de control para llevar a cabo los procedimientos de control de flujo y de errores. Finalmente, uno de los dos extremos indicará la finalización de la transmisión.

Inicio

El inicio lo puede solicitar cualquiera de los dos extremos en base a la transmisión de una de las seis órdenes previstas para fijar el modo. Esta orden tiene tres objetivos:

1. Avisa al otro extremo sobre la solicitud de la iniciación.
2. Especifica cuál de los tres modos (NRM, ABM, ARM) se está solicitando.
3. Indica si se van a utilizar números de secuencia de 3 o de 7 bits.

Si el otro extremo acepta la solicitud, la entidad HDLC transmitirá una trama de confirmación no numerada (UA, *Unnumbered Acknowledgment*) al extremo iniciante. Si la solicitud se rechaza, se envía una trama de modo desconectado (DM, *Disconnected Mode*).

Transferencia de datos

Cuando la iniciación haya sido solicitada y aceptada, se habrá establecido una conexión lógica. A partir de entonces, ambos extremos pueden comenzar a enviar datos mediante el uso de tramas-I, empezando por el número de secuencia 0. Los campos N(S) y N(R) de una trama-I contendrán los números de secuencia con los que se lleva a cabo el control de flujo y de errores. La entidad HDLC numerará la secuencia de tramas-I de forma ordenada módulo 8 o módulo 128, dependiendo de si se utilizan, respectivamente, 3 o 7 bits; para ello se usará el campo N(S). El campo N(R) se utiliza para llevar a cabo la confirmación de las tramas-I recibidas; de esta forma, se facilita que la entidad HDLC indique al otro extremo el siguiente número de trama-I que espera recibir.

Las tramas-S también se usan para controlar el flujo y los errores. La trama RR (receptor preparado) confirma la última trama-I recibida mediante la indicación de la siguiente trama-I que se espera recibir. La trama RR se usa cuando no hay tráfico (tramas-I) en sentido contrario en el que se puedan incluir las confirmaciones. La trama RNR (receptor no preparado) confirma una trama-I, como lo hace la RR, pero a la vez solicita a la entidad situada al otro extremo del enlace que suspenda la transmisión de tramas-I; cuando la entidad que envió la trama RNR esté de nuevo preparada, enviará una RR. La trama REJ (rechazo) sirve para iniciar el procedimiento ARQ con vuelta atrás N. A través de ella se indica que la última trama-I recibida se ha rechazado y, en consecuencia, se solicita la retransmisión de todas las tramas-I con números de secuencia posteriores a N(R). La trama SREJ (rechazo selectivo) se usa para solicitar la retransmisión de una única trama.

Desconexión

Cualquiera de las dos entidades HDLC pares puede iniciar la desconexión, tanto por iniciativa propia (si es que ha habido algún tipo de fallo) como tras la petición cursada por capas superiores. HDLC lleva a cabo la desconexión mediante el envío de una trama DISC (desconexión, *DISConnect*). La entidad remota puede aceptar dicha desconexión mediante la devolución de una trama UA, e informando a su capa 3 sobre la finalización de la conexión. Cualquier trama-I pendiente de confirmación puede perderse, en cuyo caso será responsabilidad de las capas superiores su recuperación.

Ejemplos de funcionamiento

Para comprender mejor el funcionamiento de HDLC, en la Figura 7.9 se presentan varios ejemplos. En los diagramas utilizados, cada flecha incluye un texto que especifica el nombre de la trama, el valor del bit P/F y, donde sea oportuno, los valores de los campos N(R) y N(S). El bit P/F se considera a valor 1 si aparece explícitamente; en caso contrario, se supondrá a valor 0.

En la Figura 7.9a se muestran las tramas involucradas en el establecimiento y desconexión del enlace. Una de las entidades HDLC envía una orden SABM a la otra e inicia un temporizador. La entidad par, tras recibir la trama SABM, devuelve una respuesta UA e inicializa las variables locales y los contadores correspondientes. La entidad que inició el enlace recibe la respuesta UA, inicia

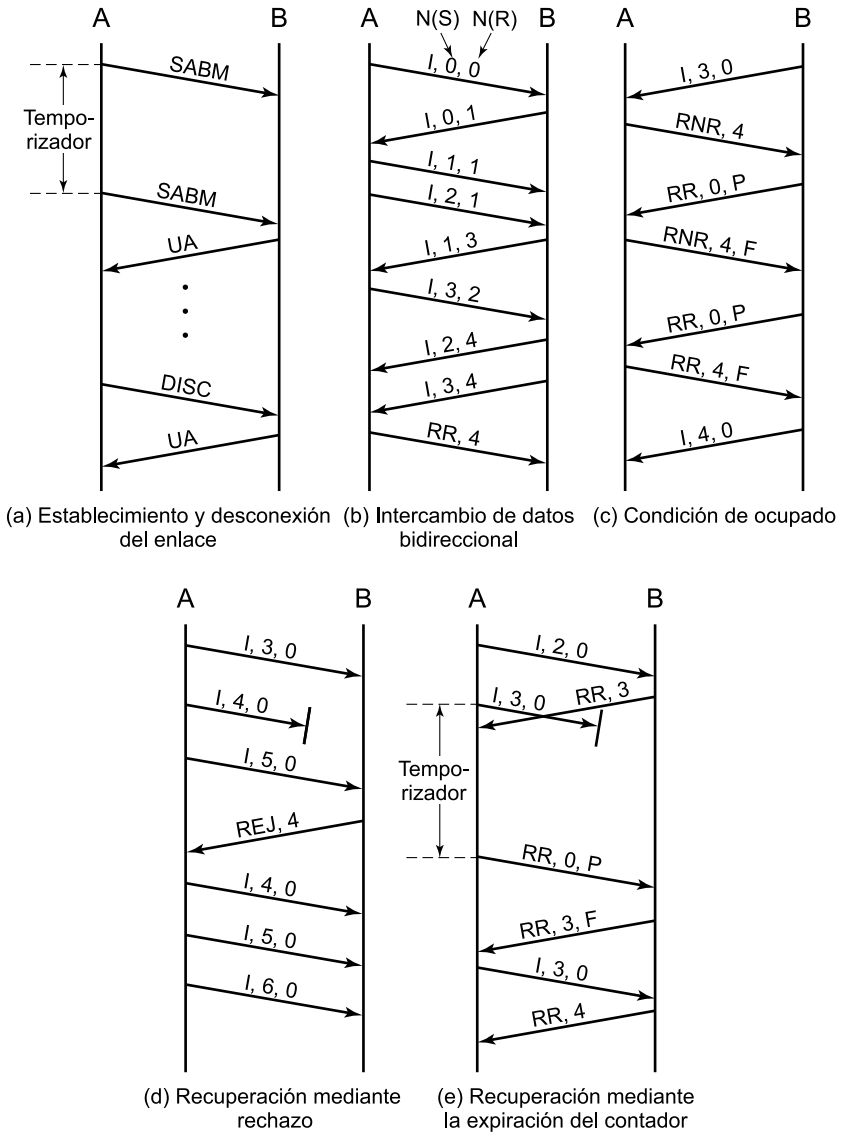


Figura 7.9. Ejemplo de funcionamiento de HDLC.

sus variables y contadores y detiene el temporizador. La conexión lógica ya está establecida, por lo que ambos extremos pueden comenzar a enviar tramas. Si el temporizador anterior expirara sin obtener la respuesta esperada, el extremo correspondiente repetirá la transmisión de la trama SABM como se indica en la figura. Este procedimiento se debe repetir hasta que se reciba una trama UA, una trama DM o hasta que, tras un cierto número de intentos, la entidad que esté intentando establecer la conexión desista e informe acerca del fallo a una entidad de gestión. En tal caso, se necesitará la intervención de las capas superiores. En la misma figura (*véase* Figura 7.9a) se muestra el procedimiento de desconexión. Uno de los dos extremos envía una orden DISC y el otro responde con una trama UA.

En la Figura 7.9b se muestra el intercambio *full-duplex* de tramas-I. Cuando una de las entidades envía una serie de tramas-I consecutivas sin que se reciban tramas de datos, el número de secuencia recibido N(R) se repetirá en todas ellas (por ejemplo, I,1,1; I,2,1 en el sentido de A a B). Cuando una entidad recibe una serie de tramas-I contiguas sin que se envíe ninguna trama, el valor del número de secuencia recibido de la siguiente trama que se emita reflejará toda esta actividad acumulada (por ejemplo, I,1,3 en el sentido de B hacia A). Obsérvese que, además de las tramas-I, el intercambio de datos puede implicar la utilización de tramas de supervisión.

En la Figura 7.9c se muestra el funcionamiento para el caso en que el receptor esté ocupado. Tal situación se presentará cuando la entidad HDLC no sea capaz de procesar las tramas-I a la velocidad a la que se reciben, o cuando el usuario no sea capaz de aceptar datos tan rápidamente. En ambos casos, la memoria temporal de la entidad receptora se desbordará, por lo que se debe detener de algún modo la recepción de tramas-I; para ello se utiliza una orden RNR. En el ejemplo, A envía una trama RNR, con la que solicita a B que detenga la transmisión de tramas-I. La estación que recibe la trama RNR sondeará, por lo general, a la estación ocupada mediante el envío periódico de tramas RR con el bit P puesto a 1. Esto exige que el otro extremo responda con una trama RR o con una RNR. Cuando la situación de ocupado cese, A devolverá una trama RR, con lo que la transmisión de tramas-I desde B se podrá reanudar.

En la Figura 7.9d se ilustra un ejemplo de recuperación de errores mediante el empleo de la orden REJ. En este ejemplo, A transmite tramas-I de número 3, 4 y 5. La número 4 sufre un error y se pierde. Cuando B recibe la trama-I número 5, la descarta debido a que su número no corresponde con el esperado, y envía una trama REJ con el campo N(R) igual a 4. Esto hará que A retransmita todas las tramas-I enviadas a partir de la 4, tras lo cual puede continuar con la transmisión de tramas adicionales.

En la Figura 7.9e se muestra un ejemplo de recuperación de un error usando los temporizadores. En este ejemplo, A transmite la trama-I número 3 como la última de una secuencia. Dicha trama sufre un error. B detecta este hecho y descarta la trama. Sin embargo, B no puede enviar una trama REJ, puesto que no hay forma de saber si se trataba de una trama-I. Si se detecta un error en una trama, todos los bits son sospechosos de ser erróneos, por lo que el receptor no sabrá qué hacer. A, sin embargo, inició un temporizador al transmitir dicha trama. Este temporizador tendrá una duración suficiente ajustada al tiempo esperado de respuesta, de modo que, si el temporizador expirase, A empezará con el procedimiento de recuperación. Este proceso se realiza, normalmente, sondeando al otro extremo mediante una orden RR con el bit P activado a fin de determinar su estado. Ya que el sondeo exige una respuesta, la entidad recibirá una trama conteniendo el campo N(R), con lo que podrá actuar en consecuencia. En el ejemplo considerado, la respuesta indica que la trama 3 se ha perdido, con lo que A procederá a retransmitirla.

Estos ejemplos no constituyen un conjunto exhaustivo de todas las posibilidades, pero resultan ilustrativos acerca del funcionamiento de HDLC.

7.4. LECTURAS RECOMENDADAS

[BERT92] ofrece un tratamiento excelente y muy detallado sobre el control de errores y de flujo. [BLAC93] proporciona una buena revisión de los protocolos para el control del enlace de datos. [FIOR95] trata algunos de los problemas relacionados con la fiabilidad de HDLC en entornos reales.

Existe una extensa bibliografía acerca del estudio de las prestaciones de los protocolos de control del enlace ARQ. Tres artículos clásicos en este sentido son [BENE64], [KONH80] y [BUX80]. En [LIN84] se presenta una revisión simplificada de los resultados sobre las prestaciones, pudiendo encontrarse un análisis más reciente en [ZORZ96]. Dos libros donde se realiza un buen estudio de las prestaciones de la capa de enlace son [SPRA91] y [WALR98].

Por su parte, [KLEI92] y [KLEI93] son dos artículos básicos donde se analizan las implicaciones que tiene el uso de velocidades del orden de gigabit en las prestaciones.

BENE64 Benice, R. «An Analysis of Retransmission Systems», *IEEE Transactions on Communication Technology*, diciembre 1964.

BERT92 Bertsekas, D., y Gallager, R. *Data Networks*. Englewood Cliffs, NJ: Prentice Hall, 1992.

BLAC93 Black, U. *Data Link Protocols*. Englewood Cliffs, NJ: Prentice Hall, 1993.

BUX80 Bux, W.; Kummerle, K.; y Truong, H. «Balanced HDLC Procedures: A Performance Analysis». *IEEE Transactions on Communications*, noviembre 1980.

FIOR95 Fiorini, D.; Chiani, M.; Tralli, V.; y Salati, C. «Can We Trust HDLC?» *Computer Communications Review*, octubre 1995.

KLEI92 Kleinrock, L. «The Latency/Bandwidth Tradeoff in Gigabit Networks». *IEEE Communications Magazine*, abril 1992.

KLEI93 Kleinrock, L. «On the Modeling and Analysis of Computer Networks». *Proceeding of the IEEE*, agosto 1993.

KONH80 Konheim, A. «A Queuing Analysis of Two ARQ Protocols», *IEEE Transactions on Communications*, julio 1980.

LIN84 Lin S.; Costello, D.; y Miller, M. «Automatic-Repeat-Request Error-Control Schemes». *IEEE Communications Magazine*, diciembre 1984.

SPRA91 Spragins, J.; Hammond, J.; y Pawlikowski, K. *Telecommunications: Protocols and Design.* Reading, MA: Addison-Wesley, 1991.

WALR98 Walrand, J. *Communication Networks*: *A First Course*. New York: McGraw-Hill, 1998.

ZORZ96 Zorzi, M., y Rao, R. «On the Use of Renewal Theory in the Analysis of ARQ Protocols». *IEEE Transactions on Communications*, septiembre 1996.

7.5. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

ARQ con vuelta atrás N
ARQ con parada y espera
ARQ con rechazo selectivo
cabecera

campo de delimitación
cola
control de errores
control de flujo
control de flujo mediante parada y espera
control de flujo mediante ventana deslizante
control del enlace de datos de alto nivel (HDLC)
enlace de datos
incorporación de confirmación (piggybacking)
protocolo de control del enlace de datos
sincronización de trama
trama de datos
transparencia en los datos

CUESTIONES DE REPASO

7.1. Enumere y defina brevemente algunos de los requisitos para una comunicación efectiva sobre un enlace de datos.

7.2. Defina el control de flujo.

7.3. Describa el esquema de control de flujo mediante parada y espera.

7.4. ¿Cuáles son las razones por las que se divide una transmisión de datos larga en tramas?

7.5. Describa el esquema de control de flujo mediante ventana deslizante.

7.6. ¿Qué ventaja presenta el control de flujo mediante ventana deslizante frente al basado en parada y espera?

7.7. ¿En qué consiste la técnica de incorporación de confirmación (*piggybacking*)?

7.8. Defina el control de errores.

7.9. Enumere elementos usuales en el control de errores llevado a cabo por parte de un protocolo de control del enlace.

7.10. Describa el procedimiento ARQ.

7.11. Enumere y defina brevemente tres versiones de ARQ.

7.12. ¿Cuáles son los tipos de estaciones soportados por HDLC? Descríbalos.

7.13. ¿Cuáles son los modos de transferencia soportados por HDLC? Descríbalos.

7.14. ¿Para qué sirve el campo de delimitación?

7.15. Defina *transparencia en los datos*.

7.16. ¿Cuáles son los tres tipos de trama soportados por HDLC? Descríbalos.

EJERCICIOS

7.1. Considérese un enlace punto a punto *half-duplex* en el que se utiliza un esquema de parada y espera y sobre el que se envía una serie de mensajes, cada uno de los cuales se segmenta en una serie de tramas. Si no se consideran errores ni bits suplementarios en las tramas:

a) ¿Qué implicaciones tiene en la utilización de la línea un aumento del tamaño de los mensajes, de forma que se necesite transmitir un menor número de ellos? El resto de elementos se mantienen fijos.

b) ¿Qué repercusión tendría en la utilización de la línea un aumento en el número de tramas, manteniendo constante el tamaño del mensaje?

c) ¿Qué sucedería con la utilización de la línea si aumentase el tamaño de las tramas?

7.2. Un canal tiene una velocidad de transmisión de 4 kbps y un retardo de propagación de 20 ms. ¿Para qué rango de tamaños de trama se conseguirá un esquema de parada y espera con una eficiencia mínima del 50%?

7.3. Supóngase el uso de tramas de 1.000 bits en un canal vía satélite a 1 Mbps con 270 ms de retardo. Calcule la utilización máxima de la línea para:

a) Un esquema de control del flujo mediante parada y espera.

b) Un esquema de control del flujo continuo con un tamaño de ventana igual a 7.

c) Un esquema de control del flujo continuo con un tamaño de ventana igual a 127.

d) Un esquema de control del flujo continuo con un tamaño de ventana igual a 255.

7.4. En la Figura 7.10, el nodo A genera tramas que se envían al nodo C a través del nodo B. Determine la velocidad de transmisión mínima entre los nodos B y C de manera que la memoria temporal del nodo B no se sature, teniendo en cuenta que:

La velocidad de transmisión entre A y B es 100 kbps.

El retardo de propagación es 5 μs/km para ambas líneas.

Existen líneas *full-duplex* entre los nodos.

Todas las tramas de datos tienen una longitud de 1.000 bits y se hace uso de tramas ACK independientes de longitud despreciable.

Entre A y B se usa un protocolo de ventana deslizante con tamaño de ventana igual a 3.

Entre B y C se usa un protocolo de parada y espera.

No hay errores.

Sugerencia: para no saturar la memoria temporal de B, el número medio de tramas entrantes en dicho nodo debe ser igual, a lo largo de un intervalo grande, al número medio de tramas salientes.

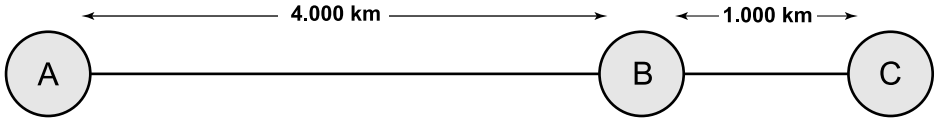


Figura 7.10. Configuración para el Ejercicio 7.4.

7.5. Un canal tiene una velocidad de transmisión de R bps y un retardo de propagación de t s/km. La distancia entre los nodos emisor y receptor es de L kilómetros. Los nodos intercambian tramas de longitud fija igual a B bits. Obtenga una expresión que proporcione el tamaño mínimo del campo de numeración de secuencia de trama en función de R, t, B y L (considerando la utilización máxima). Supóngase que las tramas ACK tienen un tamaño despreciable y que el procesamiento en los nodos es instantáneo.

7.6. En el estudio del esquema ARQ con parada y espera no se ha hecho mención a las tramas de rechazo (REJ) ¿Por qué no es necesario utilizar REJ0 y REJ1 en un ARQ con parada y espera?

7.7. Supóngase el empleo de un esquema ARQ con rechazo selectivo con $W = 4$. Muestre mediante un ejemplo que se necesita una numeración de secuencia de 3 bits.

7.8. Considerando las mismas suposiciones que las adoptadas en la Figura 7.13 del Apéndice 7.A, represente la utilización de la línea en función de P, la probabilidad de que una única trama sea errónea, para los siguientes procedimientos de control de errores:

a) Parada y espera.

b) Vuelta atrás N con $W = 7$.

c) Vuelta atrás N con $W = 127$.

d) Rechazo selectivo con $W = 7$.

e) Rechazo selectivo con $W = 127$.

Para las situaciones anteriores considérense los siguientes valores de a: 0,1, 1, 10, 100. Obtenga las conclusiones pertinentes acerca de cuál es la técnica más adecuada para los distintos valores de a.

7.9. Dos nodos vecinos (A y B) usan un protocolo de ventana deslizante de 3 bits para los números de secuencia. Se utiliza como procedimiento ARQ un vuelta atrás N con un tamaño de ventana igual a 4. Suponiendo que A transmite y B recibe, muestre las distintas posiciones de las ventanas para la siguiente sucesión de eventos:

a) Antes de que A envíe ninguna trama.

b) Después de que A envíe las tramas 0, 1 y 2 y reciba las confirmaciones de B correspondientes a las tramas 0 y 1.

c) Después de que A envíe las tramas 3, 4, y 5, B confirme la 4 y la trama ACK correspondiente se reciba en A.

7.10. En el procedimiento ARQ con rechazo selectivo no se pueden usar confirmaciones desordenadas. Es decir, si la estación X rechaza la trama i, todas las tramas-I y RR siguientes enviadas por X deben tener $N(R) = i$ hasta que la trama i se reciba correctamente, incluso en el caso de que, mientras tanto, se recibiesen sin errores otras tramas con $N(S) > i$. Una posible mejora es la siguiente: una trama-I o una RR con $N(R) = j$ se interpretará como que la trama $j - 1$ y todas las precedentes han sido aceptadas, excepto aquellas que hayan sido rechazadas explícitamente mediante una trama SREJ. Discuta los posibles problemas que plantea este procedimiento.

7.11. El estándar ISO para los procedimientos HDLC (ISO 4335) incluye las siguientes definiciones: (1) una situación de rechazo (REJ) se considera finalizada cuando se recibe una trama-I con el campo N(S) igual al N(R) de la trama REJ de salida; y (2) una situación de rechazo selectivo (SREJ) se considera finalizada cuando se recibe una trama-I con el campo N(S) igual al N(R) de la trama SREJ. El estándar incluye reglas relativas a la relación entre las tramas REJ y SREJ. Estas reglas indican qué es admisible (en términos de transmisión de tramas REJ y SREJ) si una situación REJ o una SREJ no ha finalizado. Deduzca las reglas y justifique la respuesta.

7.12. Dos estaciones se comunican a través de un enlace de satélite a 1 Mbps con un retardo de propagación de 270 ms. El satélite se limita a retransmitir de una estación a otra los datos recibidos, con un retardo de conmutación despreciable. Si se usan tramas HDLC de 1.024 bits con números de secuencia de 3 bits, ¿cuál será el rendimiento máximo posible?; es decir, ¿cuál es el rendimiento de los bits de datos transportados en las tramas HDLC?

7.13. Es evidente que en una trama HDLC se necesita la inserción de bits en los campos de dirección, datos y FCS. ¿Es necesaria en el campo de control?

7.14. Proponga posibles mejoras al algoritmo de inserción de bits para evitar los problemas existentes cuando aparecen errores que afectan a un solo bit.

7.15. Haciendo uso de la secuencia de bits de ejemplo dada en la Figura 7.8, muestre la señal correspondiente a una codificación NRZ-L ¿Le sugiere esto alguna ventaja de la inserción de bits?

7.16. Suponga que una estación primaria HDLC en modo NRM envía seis tramas-I a una secundaria. El campo N(S) de la primaria es tres (011 en binario) antes de enviar las seis tramas. Si el bit P está activado en la sexta trama, ¿cuál será el valor del campo N(R) devuelto por la secundaria tras la última trama? Suponga que no hay errores.

7.17. Supóngase que se dispone de varios enlaces físicos para conectar dos estaciones. Se utiliza un «HDLC multienlace» con el que se hace un uso eficiente de estos enlaces mediante el envío de tramas de acuerdo a una estrategia FIFO (*First In First Out*) utilizando el siguiente enlace disponible ¿Qué mejoras es preciso introducir en HDLC?

7.18. Un servidor WWW (World Wide Web) está diseñado usualmente para recibir mensajes relativamente pequeños generados por sus clientes, pero para transmitir mensajes potencialmente muy largos hacia ellos. Explique qué tipo de protocolo ARQ (rechazo selectivo o vuelta atrás N) provocaría menos carga en un servidor WWW dado.

APÉNDICE 7.A. ANÁLISIS DE PRESTACIONES

En este apéndice se lleva a cabo un análisis de prestaciones de los esquemas de control de flujo mediante ventana deslizante.

CONTROL DE FLUJO MEDIANTE PARADA Y ESPERA

Calculemos la máxima eficiencia potencial de una línea punto a punto *half-duplex* donde se usa el esquema de parada y espera descrito en la Sección 7.1. Supóngase que se va a enviar un mensaje largo en base a una serie de tramas F_1, F_2, ..., F_n, de la siguiente manera:

- La estación S_1 envía F_1.
- La estación S_2 envía una confirmación.
- La estación S_1 envía F_2.
- La estación S_2 envía una confirmación.

$$\vdots$$

- La estación S_1 envía F_n.
- La estación S_2 envía una confirmación.

El tiempo total para enviar los datos, T, se puede expresar como $T = nT_F$, donde T_F es el tiempo en enviar una trama y recibir la confirmación. T_F se puede expresar de la siguiente manera:

$$T_F = t_{\text{prop}} + t_{\text{trama}} + t_{\text{prop}} + t_{\text{prop}} + t_{\text{ack}} + t_{\text{prop}}$$

donde

t_{prop} = tiempo de propagación de S_1 a S_2.

t_{trama} = tiempo en transmitir una trama (tiempo que tarda el emisor en enviar todos los bits de la trama).

t_{proc} = tiempo de procesamiento que tarda una estación en reaccionar a un evento de entrada.

t_{ack} = tiempo en transmitir una confirmación.

Supóngase que el tiempo de procesamiento es despreciable en términos relativos y que la trama de confirmación es muy pequeña comparada con la de datos. Ambas suposiciones son razonables, con lo que el tiempo total involucrado en el envío de los datos se puede expresar como

$$T = n(2t_{prop} + t_{trama})$$

De ese tiempo, sólo se emplea realmente $n \times t_{trama}$ en transmitir datos; el resto es suplementario. La utilización, o eficiencia, de la línea es:

$$U = \frac{n \times t_{trama}}{n(2t_{prop} + t_{trama})} = \frac{t_{trama}}{2t_{prop} + t_{trama}} \tag{7.3}$$

Es útil definir el parámetro $a = t_{prop}/t_{trama}$ (*véase* Figura 7.2), de modo que

$$U = \frac{1}{1 + 2a} \tag{7.4}$$

Ésta es la utilización máxima posible de la línea. Dado que la trama contiene bits suplementarios, la utilización real será inferior. El parámetro a es constante si tanto t_{prop} como t_{trama} lo son, lo cual es la situación más habitual: por lo general se utilizan tramas de longitud fija y, además, el retardo de propagación es constante para enlaces punto a punto.

Para aclarar un poco más la Ecuación (7.4), consideremos una expresión diferente para el parámetro a. Sea

$$a = \frac{\text{Tiempo de propagación}}{\text{Tiempo de transmisión}} \tag{7.5}$$

El tiempo de propagación es igual a la distancia del enlace, d, dividida por la velocidad de propagación, V. Para transmisiones no guiadas a través del aire o el espacio, V es la velocidad de la luz, aproximadamente igual a 3×10^8 m/s. Para transmisiones guiadas (fibra óptica y medios de cobre), V es aproximadamente igual a 0,67 veces la velocidad de la luz. El tiempo de transmisión es igual a la longitud de la trama en bits, L, dividida por la velocidad de transmisión, R. Por tanto,

$$a = \frac{d/V}{L/R} = \frac{Rd}{VL}$$

Luego, para tramas de longitud fija, a es proporcional a la velocidad de transmisión multiplicada por la longitud del medio. Una forma útil de interpretar el parámetro a es ver éste como la relación entre la longitud del medio en bits $\left[R \times \left(\frac{d}{V}\right)\right]$, y la longitud de la trama, L.

Teniendo presente esta interpretación, en la Figura 7.2 se ilustra la Ecuación (7.4). En esta figura se normaliza el tiempo de transmisión a la unidad, siendo, por tanto, el tiempo de propagación, según la Ecuación (7.5), igual a a. Para el caso $a < 1$, la longitud del enlace en bits es menor que la de la trama. La estación T empieza a transmitir una trama en el instante de tiempo t_0. En $t_0 + a$, el primer bit de la trama llega a la estación receptora R, encontrándose T transmitiendo la trama aún. En $t_0 + 1$, T concluye la transmisión. En $t_0 + 1 + a$, R habrá recibido la trama completa, e inmediatamente después transmitirá una pequeña trama de confirmación. Esta confirmación llega a T en $t_0 + 1 + 2a$. El tiempo total transcurrido es $1 + 2a$, mientras que el tiempo de transmisión es 1. Por tanto, la utilización será $1/(1 + 2a)$. Como se muestra en la Figura 7.2, el mismo resultado se obtiene para $a > 1$.

Ejemplo 7.3. Consideremos en primer lugar una red de área amplia (WAN) basada en ATM (*Asynchronous Transfer Mode*, descrita en la Parte III), con dos estaciones separadas mil kilómetros. El tamaño estandarizado de las tramas ATM (denominadas celdas) es 424 bits y una de las velocidades de transmisión normalizadas en este sistema es 155,52 Mbps. Por tanto, el tiempo de transmisión es igual a $424/(155{,}52 \times 10^6) = 2{,}7 \times 10^{-6}$ segundos. Si se supone un enlace de fibra óptica, el tiempo de propagación resulta $(10^6 \text{ m})/(2 \times 10^8 \text{ m/s}) = 0{,}5 \times 10^{-2}$ segundos. Así pues, $a = (0{,}5 \times 10^{-2})/(2{,}7 \times 10^{-6}) \approx 1.850$, por lo que la eficiencia es sólo $1/3.701 = 0{,}00027$.

En términos de distancia, el otro caso extremo corresponde a una red de área local (LAN). Las distancias aquí manejadas varían entre 0,1 y 10 km, con velocidades de transmisión comprendidas entre 10 Mbps y 1 Gbps; las velocidades superiores se tienden a asociar con las distancias más cortas. Usando un valor de $V = 2 \times 10^8$ m/s, un tamaño de trama de 1.000 bits y una velocidad de transmisión igual a 10 Mbps, resulta un valor de a en el rango de 0,005 a 0,5. Esto implica una utilización comprendida entre 0,5 y 0,99. Para una LAN a 100 Mbps, se puede obtener una utilización comparable si se consideran distancias más cortas.

Se puede observar que las LAN son generalmente bastante eficientes, no ocurriendo lo mismo con las WAN de alta velocidad. Como último ejemplo, considérese una transmisión digital de datos vía módem sobre una línea telefónica. Una velocidad de datos típica en este caso es 56 kbps. Supongamos de nuevo una longitud de trama de 1.000 bits, pudiendo estar comprendida la longitud del enlace entre unas pocas decenas de metros y varios miles de kilómetros. Si consideramos una distancia corta, digamos $d = 1.000$ m, entonces $a = (56.000 \text{ bps} \times 1.000 \text{ m})/(2 \times 10^8 \text{ m/s} \times 1.000 \text{ bits}) = 2{,}8 \times 10^{-4}$ y la eficiencia será igual a 1,0. En caso de que la distancia sea elevada, por ejemplo $d = 5.000$ km, tendremos $a = (56.000 \times 5 \times 10^6)/(2 \times 10^8 \times 1.000) = 1{,}4$ y la eficiencia será igual a 0,26.

CONTROL DE FLUJO SIN ERRORES MEDIANTE VENTANA DESLIZANTE

En el esquema de control de flujo mediante ventana deslizante, la eficiencia de la línea depende tanto del tamaño de la ventana W, como del valor de a. Por comodidad, normalizaremos de nuevo el tiempo de transmisión de la trama a la unidad, por lo que el tiempo de propagación será igual a a. En la Figura 7.11 se muestra la eficiencia de una línea punto a punto *full-duplex*[2]. La estación A empieza a transmitir una serie de tramas en $t = 0$. El primer bit de la primera trama llega a la estación B en $t = a$. La primera trama se recibe completamente en $t = a + 1$. Suponiendo un tiempo

[2] Por sencillez, supondremos que a es un valor entero, de forma que en la línea cabrá un numero entero de tramas. Este argumento es igualmente válido para valores de a no enteros.

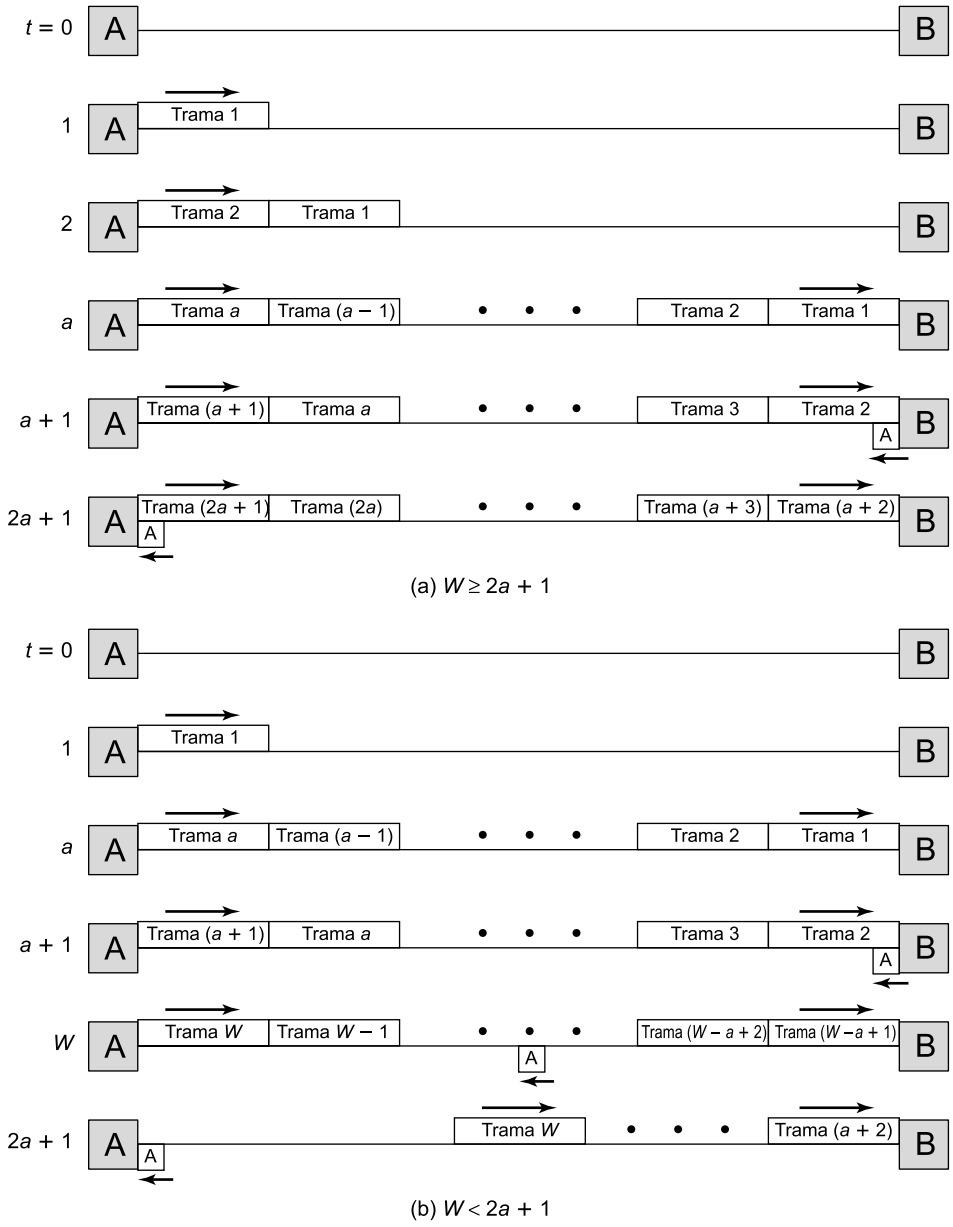


Figura 7.11. Temporización en el protocolo de ventana deslizante.

de procesamiento despreciable, B confirmará inmediatamente la primera trama (ACK). Supóngase también que la trama de confirmación es tan pequeña que el tiempo de transmisión asociado es despreciable. Entonces, la trama ACK llegará a A en $t = 2a + 1$. Para evaluar las prestaciones es preciso considerar dos casos:

- **Caso 1:** $W \geqslant 2a + 1$. La confirmación de la trama 1 llega a A antes de que ésta agote su ventana. Por tanto, A puede transmitir continuamente sin pausa, de modo que la utilización será 1,0.

- **Caso 2:** $W < 2a + 1$. A agota su ventana en $t = W$ y no podrá enviar tramas adicionales hasta $t = 2a + 1$. Por tanto, la utilización de la línea es W unidades de tiempo por cada periodo de $(2a + 1)$ unidades de tiempo.

Por tanto, podemos expresar la utilización como

$$U = \begin{cases} 1 & W \geqslant 2a + 1 \\ \dfrac{W}{2a + 1} & W < 2a + 1 \end{cases} \tag{7.6}$$

Generalmente, el número de secuencia se especifica mediante un campo de n-bits, siendo el tamaño máximo de la ventana $W = 2^n - 1$ (no 2^n, como se explicó en la Sección 7.2). En la Figura 7.12 se muestra la máxima utilización que puede conseguirse para ventanas de tamaño 1, 7 y 127, en función de a. Una ventana de tamaño 1 corresponde con un esquema de parada y espera. Una ventana de tamaño igual a 7 (3 bits) resulta adecuada para diversas aplicaciones, mientras que una de tamaño 127 (7 bits) es útil para valores grandes de a (como los que se pueden encontrar en redes WAN de alta velocidad).

ARQ

Ya se ha comentado que el control de flujo mediante ventana deslizante es más eficiente que el de parada y espera. Es de esperar que, si se incorporan procedimientos para el control de los errores, esto seguirá siendo cierto; es decir, que las técnicas ARQ mediante vuelta atrás N y mediante rechazo selectivo son más eficientes que el esquema ARQ con parada y espera. Desarrollemos algunas expresiones para determinar la mejora que cabe esperar.

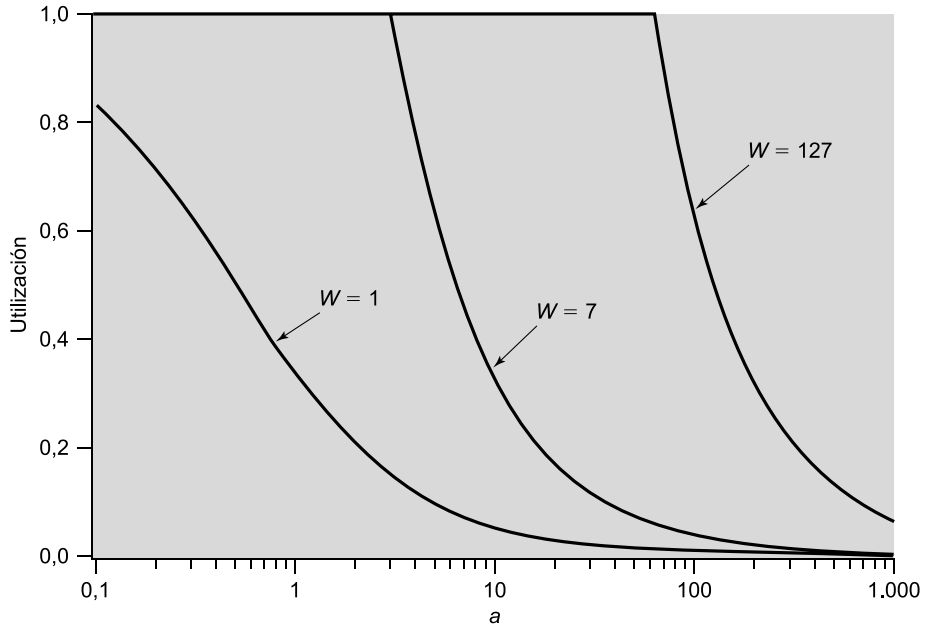


Figura 7.12. Utilización conseguida mediante el esquema de ventana deslizante en función de *a*.

Considérese en primer lugar un esquema ARQ con parada y espera. Si no hay errores, la utilización máxima es $1/(1 + 2a)$, como se indica en la Ecuación (7.4). Supóngase ahora que existen algunas tramas repetidas debido a la aparición de errores. Para comenzar, obsérvese que la utilización U se puede definir como

$$U = \frac{T_f}{T_t} \tag{7.7}$$

donde

T_f = tiempo empleado por el emisor para transmitir una trama.

T_t = tiempo total durante el cual la línea está ocupada enviando una única trama.

Para el caso sin errores usando ARQ con parada y espera,

$$U = \frac{T_f}{T_f + 2T_p}$$

donde T_p es el tiempo de propagación. Dividiendo por T_f y recordando que $a = T_p/T_f$, se obtiene de nuevo la Ecuación (7.4). Si hay errores, se debe modificar la Ecuación (7.7) de la siguiente manera:

$$U = \frac{T_f}{N_r T_t}$$

donde N_r es el valor esperado del número de transmisiones por trama. Por tanto, en ARQ con parada y espera se tiene que:

$$U = \frac{1}{N_r(1 + 2a)}$$

Se puede obtener una expresión sencilla para N_r considerando la probabilidad P de que sólo una trama sea errónea. Si se supone que las tramas ACK y NAK están libres de error, la probabilidad de que se necesiten exactamente k intentos para transmitir con éxito una trama es $P^{k-1}(1 - P)$. Es decir, se tendrán $(k - 1)$ intentos infructuosos seguidos de un intento con éxito; la probabilidad de que esto ocurra es justo el producto de las probabilidades de los eventos individuales. Entonces[3]

$$N_r = E[\text{transmisiones}] = \sum_{i=1}^{\infty} (i \times \Pr[i \text{ transmisiones}]) = \sum_{i=1}^{\infty} (iP^{i-1}(1 - P)) = \frac{1}{1 - P}$$

De modo que se tiene:

Parada y espera: $U = \dfrac{1 - P}{1 + 2a}$

Para un protocolo de ventana deslizante se aplica la Ecuación (7.6) en caso de que no existan errores. En el esquema ARQ con rechazo selectivo se puede utilizar el mismo razonamiento que el

[3] Para obtener esta expresión se usa la igualdad $\sum_{i=1}^{\infty} (iX^{i-1}) = \dfrac{1}{(1 - X^2)}$ para $(-1 < X < 1)$.

seguido en el ARQ con parada y espera. Es decir, las ecuaciones correspondientes a la situación en que no existan errores se deben dividir por N_r, donde, de nuevo, $N_r = 1/(1 - P)$. Por tanto,

$$\textbf{Rechazo selectivo:} \quad U = \begin{cases} 1 - P & W(1 - P) \geqslant 2a + 1 \\ \dfrac{W(1 - P)}{2a + 1} & W < 2a + 1 \end{cases}$$

El mismo razonamiento se puede aplicar al esquema ARQ con vuelta atrás N, si bien en este caso hemos de ser más cuidadosos al aproximar N_r. Por cada error es preciso retransmitir K tramas, en lugar de una sola como se ha considerado hasta ahora. Por tanto,

$$N_r = E[\text{número de tramas transmitidas para conseguir una correcta}] = \sum_{i=1}^{\infty} f(i)P^{i-1}(1 - P)$$

donde $f(i)$ es el número total de tramas transmitidas si la trama original se debe transmitir i veces. Esto se expresa de la siguiente manera

$$f(i) = 1 + (i - 1)K = (1 - K) + Ki$$

Sustituyendo, se obtiene[4]

$$N_r = (1 - K) \sum_{i=1}^{\infty} P^{i-1}(1 - P) + K \sum_{i=1}^{\infty} iP^{i-1}(1 - P) = 1 - K + \frac{K}{1 - P} = \frac{1 - P + KP}{1 - P}$$

Analizando la Figura 7.11, el lector puede concluir que K es aproximadamente igual a $(2a + 1)$ para el caso $W \geqslant (2a + 1)$, y $K = W$ si $W < (2a + 1)$. Por tanto,

$$\textbf{Vuelta atrás N:} \quad U = \begin{cases} \dfrac{1 - P}{1 + 2aP} & W \geqslant 2a + 1 \\ \dfrac{W(1 - P)}{(2a + 1)(1 - P + WP)} & W < 2a + 1 \end{cases}$$

Obsérvese que para $W = 1$, los esquemas ARQ con rechazo selectivo y con vuelta atrás N quedan reducidos al de parada y espera. En la Figura 7.13[5] se comparan las tres técnicas de control de errores para un valor $P = 10^{-3}$. Tanto esta figura como las ecuaciones son sólo aproximaciones. Así, por ejemplo, no se ha considerado la ocurrencia de errores en las tramas de confirmación y, en el caso del procedimiento vuelta atrás N, no se ha tenido en cuenta la posibilidad de aparición de errores en las tramas retransmitidas. No obstante, los resultados mostrados dan una buena idea acerca de las prestaciones relativas de las tres técnicas estudiadas.

---

[4] Para obtener esta expresión se usa la igualdad $\sum_{i=1}^{\infty} X^{i-1} = \dfrac{1}{(1 - X)}$ para $(-1 < X < 1)$.

[5] Las curvas correspondientes a los esquemas vuelta atrás N y rechazo selectivo están tan próximas entre sí en el caso $W = 7$, que parecen la misma en la figura.

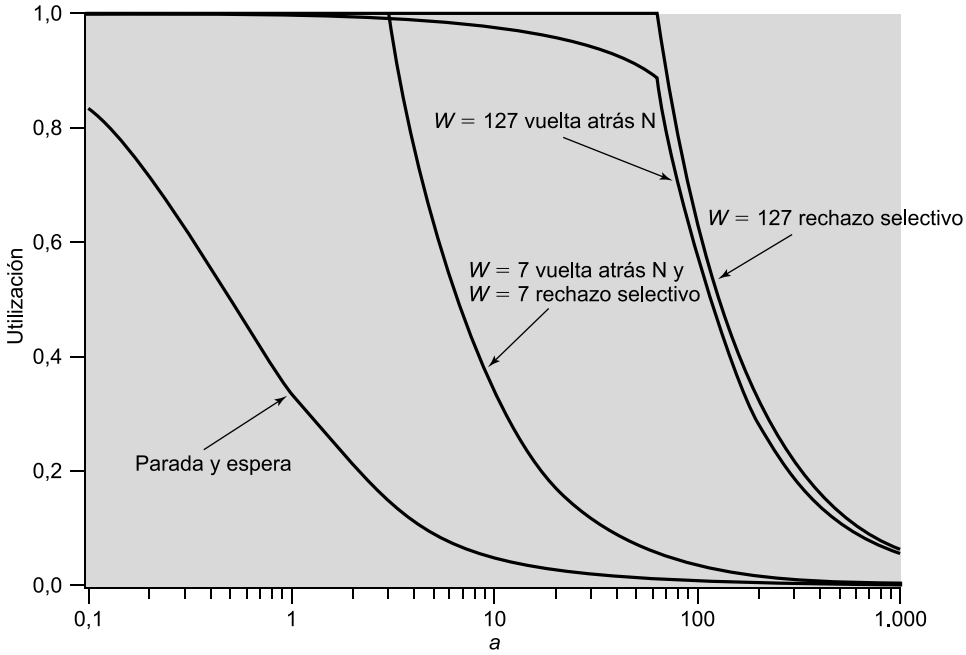


Figura 7.13. Utilización conseguida mediante los esquemas ARQ en función del parámetro a ($P = 10^{-3}$).

CAPÍTULO 8

Multiplexación

8.1. Multiplexación por división en frecuencias
Características
Sistemas de portadora analógica
Multiplexación por división en la longitud de onda

8.2. Multiplexación por división en el tiempo síncrona
Características
Control del enlace en TDM
Sistemas de portadora digital
SONET/SDH

8.3. Multiplexación por división en el tiempo estadística
Características
Prestaciones
Cable-módem

8.4. Línea de abonado digital asimétrica
Diseño ADSL
Multitono discreto

8.5. xDSL
Línea de abonado digital de alta velocidad (HDSL)
Línea de abonado digital de una sola línea (SDSL)
Línea de abonado digital de muy alta velocidad (VDSL)

8.6. Lecturas y sitios web recomendados

8.7. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- Para hacer un uso eficiente de las líneas de telecomunicaciones de alta velocidad se emplean técnicas de multiplexación, las cuales permiten que varias fuentes de transmisión compartan una capacidad de transmisión superior. Las dos formas usuales de multiplexación son las de división en frecuencias (FDM, *Frequency-Division Multiplexing*) y división en el tiempo (TDM, *Time-Division Multiplexing*).
- La **multiplexación por división en frecuencias** se puede usar con señales analógicas, de modo que se transmiten varias señales a través del mismo medio gracias a la asignación de una banda de frecuencia diferente para cada señal. El equipamiento de modulación es preciso para desplazar cada señal a la banda de frecuencia requerida, siendo necesarios, por su parte, los equipos de multiplexación para combinar las señales moduladas.
- La **multiplexación por división en el tiempo síncrona** se puede utilizar con señales digitales o con señales analógicas que transportan datos digitales. En esta forma de multiplexación, los datos procedentes de varias fuentes se transmiten en tramas repetitivas. Cada trama consta de un conjunto de ranuras temporales, asignándosele a cada fuente una o más ranuras por trama. El efecto obtenido es la mezcla de los bits de datos de las distintas fuentes.
- La **multiplexación por división en el tiempo estadística** proporciona un servicio generalmente más eficiente que la técnica TDM síncrona para el soporte a terminales. Las ranuras temporales en TDM estadística no están preasignadas a fuentes de datos concretas, sino que los datos de usuario se almacenan y transmiten tan rápido como es posible haciendo uso de las ranuras temporales disponibles.

En el Capítulo 7 se llevó a cabo una descripción de técnicas eficientes para hacer uso de un enlace de datos en condiciones de alta carga. En particular, con dos dispositivos conectados mediante un enlace punto a punto es deseable, por lo general, emitir múltiples tramas de modo que el enlace no constituya un cuello de botella entre las estaciones. Considérese a continuación la situación contraria. Normalmente, dos estaciones de comunicaciones no utilizan toda la capacidad de un enlace de datos; con objeto de mejorar la eficiencia sería posible compartir esta capacidad. Un concepto general para tal compartición es el de *multiplexación*.

Una aplicación usual de la multiplexación son las comunicaciones de larga distancia. Los enlaces de las redes de larga distancia son líneas de alta capacidad de fibra, de cable coaxial o de microondas, de modo que pueden transportar simultáneamente varias transmisiones de voz y de datos haciendo uso de las técnicas de multiplexación.

La Figura 8.1 muestra la función de multiplexación en su forma más simple. Existen n entradas a un multiplexor, que se conecta a un demultiplexor mediante un único enlace de datos. El enlace es capaz de transportar n canales de datos independientes. El multiplexor combina (multiplexa) los datos de las n líneas de entrada y los transmite a través de un enlace de datos de capacidad superior. Por su parte, el demultiplexor capta la secuencia de datos multiplexados, separa (demultiplexa) los datos de acuerdo con el canal y los envía hacia las líneas de salida correspondientes.

El amplio uso de las técnicas de multiplexación en comunicaciones de datos se puede explicar como sigue:

- A medida que la velocidad aumenta, la transmisión es más efectiva desde el punto de vista del coste. Es decir, para una aplicación y distancia dadas, el coste por kbps decrece con el

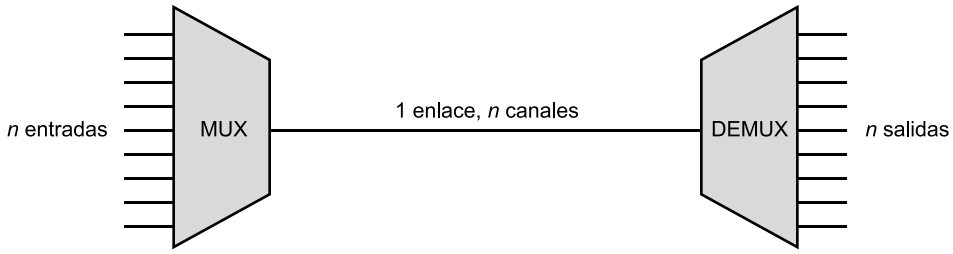


Figura 8.1. Multiplexación.

incremento en la velocidad de transmisión de datos. De forma análoga, el coste de los equipos de transmisión y recepción, por kbps, decrece con el aumento de la velocidad.

- La mayor parte de los dispositivos de comunicación de datos requieren velocidades de datos relativamente bajas. Por ejemplo, para la mayoría de las aplicaciones de terminales y de computadores personales no relacionadas con acceso web ni uso intensivo de gráficos, resulta adecuada por lo general una velocidad comprendida entre 9.600 bps y 64 kbps.

Los puntos anteriores se refieren a dispositivos de comunicación de datos, pudiéndose aplicar también a comunicaciones de voz. Es decir, cuanto mayor sea la capacidad de la transmisión, en términos de canales de voz, menor será el coste por canal de voz individual, siendo reducida la capacidad requerida por cada canal de voz.

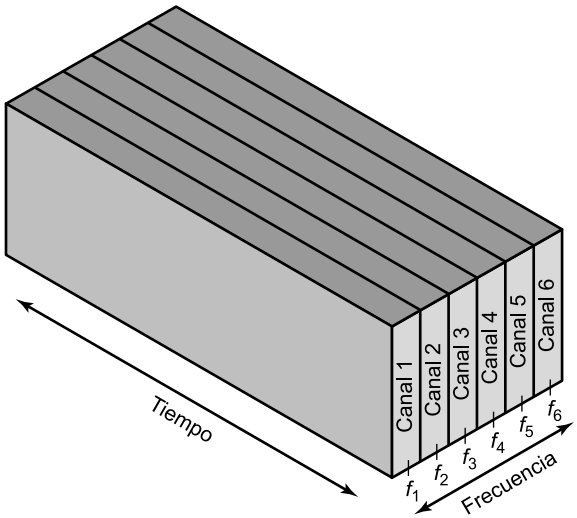
Este capítulo centra su interés en tres tipos de técnicas de multiplexación. La primera, multiplexación por división en frecuencias (FDM), es la más utilizada, resultando familiar para quienes hayan usado una radio o una televisión. La segunda es un caso particular de la multiplexación por división en el tiempo (TDM), conocida como TDM síncrona. Ésta se emplea generalmente para multiplexar secuencias de voz digitalizadas y secuencias de datos. El tercer tipo persigue la mejora en la eficiencia de la técnica TDM síncrona haciendo más complejo el multiplexor. Esta técnica se conoce con varios nombres, entre los que se encuentran TDM estadística, TDM asíncrona y TDM inteligente. En este texto se emplea el término *TDM estadística*, resaltándose así una de sus propiedades principales. Finalmente se estudiará el bucle de abonado digital, que combina las tecnologías FDM y TDM síncrona.

8.1. MULTIPLEXACIÓN POR DIVISIÓN EN FRECUENCIAS

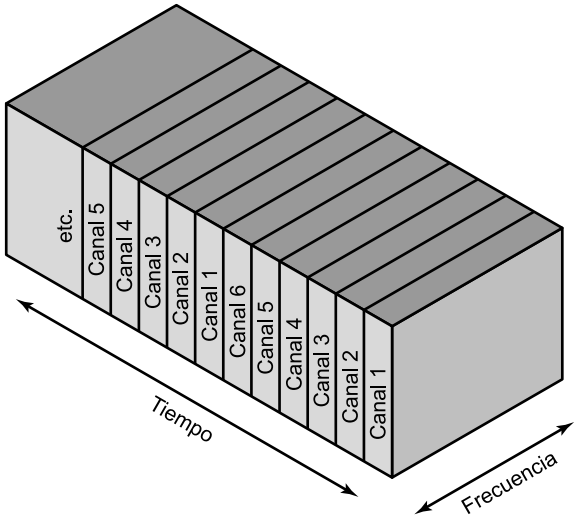
CARACTERÍSTICAS

Es posible utilizar FDM cuando el ancho de banda útil del medio de transmisión supera el ancho de banda requerido por las señales a transmitir. Se pueden transmitir varias señales simultáneamente si cada una de ellas se modula con una frecuencia portadora diferente y las frecuencias portadoras están suficientemente separadas para que los anchos de banda de las señales no se solapen de forma importante. En la Figura 8.2a se muestra un caso general de FDM. En ella se considera la entrada de seis líneas a un multiplexor, el cual modula cada señal a una frecuencia diferente (f_1, ..., f_6). Cada señal modulada precisa un cierto ancho de banda centrado alrededor de su frecuencia portadora y conocido como **canal**. Para evitar interferencias, los canales se separan mediante bandas guardas o de seguridad, las cuales son zonas no utilizadas del espectro.

La señal compuesta transmitida a través del medio es analógica. Sin embargo, hemos de indicar que las señales de entrada pueden ser tanto digitales como analógicas. En el primer caso, las seña-



(a) Multiplexación por división en frecuencias



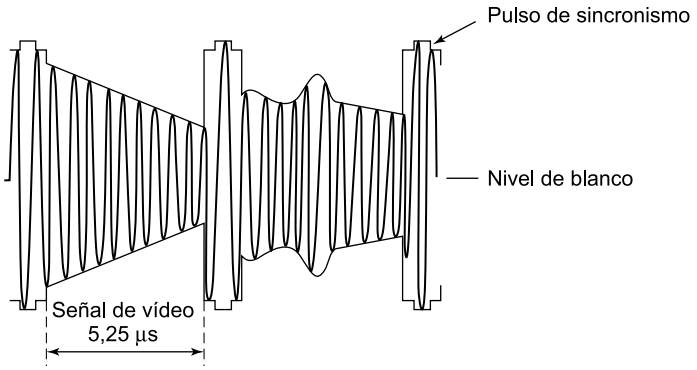
(b) Multiplexación por división en el tiempo

Figura 8.2. FDM y TDM.

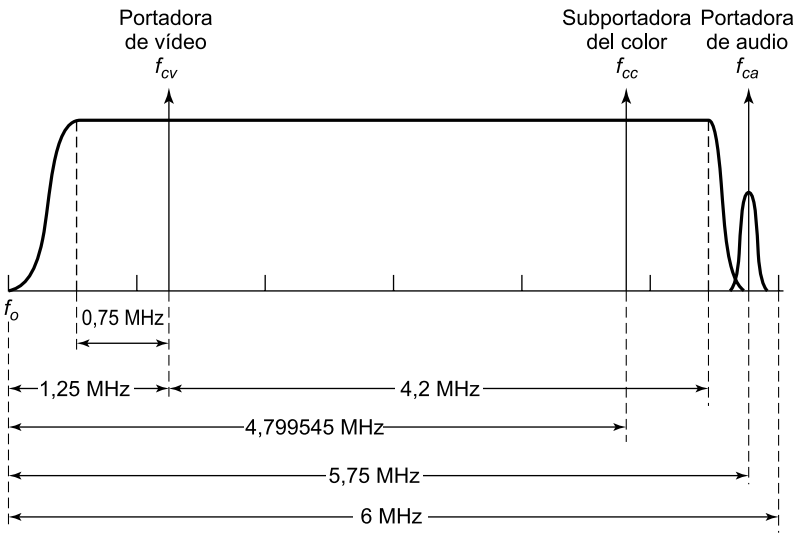
les se deben hacer pasar previamente a través de un módem para ser convertidas en analógicas. En cualquier caso, la señal de entrada analógica se debe modular para trasladarla a la banda de frecuencia apropiada.

Ejemplo 8.1. Un ejemplo familiar de FDM es la televisión convencional (de difusión) y por cable. La señal de televisión estudiada en el Capítulo 3 ocupa un ancho de banda de 6 MHz. La Figura 8.3 muestra la señal de TV transmitida y su ancho de banda. La señal de vídeo en blanco y negro se modula en AM con una portadora f_{cv}. Dado que la señal de vídeo en banda base tiene un ancho de banda de 4 MHz, es de esperar que la señal modulada ocupe un ancho de

banda de 8 MHz centrado en torno a f_{cv}. Para ahorrar ancho de banda, la señal se hace pasar por un filtro de banda lateral con objeto de suprimir la mayor parte de la banda lateral inferior. La señal resultante se extiende desde aproximadamente los $f_{cv} - 0{,}75$ MHz hasta los $f_{cv} + 4{,}2$ MHz. Para transmitir información correspondiente al color se usa una subportadora de color independiente, f_{cc}, la cual estará lo suficientemente alejada de f_{cv} para evitar la existencia de interferencias importantes. Finalmente, la señal de audio se modula a f_{ca}, fuera del ancho de banda efectivo de las otras dos señales. Para la señal de audio se reserva un ancho de banda de 50 kHz. La señal compuesta cabe en un ancho de banda de 6 MHz, con las portadoras de vídeo, color y audio a 1,25 MHz, 4,799545 MHz y 5,75 MHz por encima del extremo inferior de la banda, respectivamente. Así pues, haciendo uso de FDM se pueden multiplexar varias señales de TV en un cable CATV, cada una de ellas con un ancho de banda de 6 MHz. Dado el enorme ancho de banda de un cable coaxial (hasta 500 MHz), haciendo uso de FDM se pueden transmitir simultáneamente docenas de señales de TV. Está claro que la propagación en radiofrecuencia a través de la atmósfera es también una forma de FDM.



(a) Modulación en amplitud de la señal de vídeo



(b) Magnitud del espectro de la señal de RF de vídeo

Figura 8.3. Señal de TV transmitida.

En la Figura 8.4 se muestra un esquema general de un sistema FDM. Se multiplexan varias señales analógicas o digitales [$m_i(t)$, $i = 1, n$] a través del mismo medio de transmisión. Para ello, cada señal $m_i(t)$ se modula mediante una portadora f_i. Dado que se usan varias portadoras, cada una de ellas se denomina **subportadora**, pudiéndose hacer uso de cualquier tipo de modulación. Las señales moduladas analógicas resultantes se suman para dar lugar a una señal $m_b(t)$ en banda base compuesta[1]. En la Figura 8.4b se muestra el resultado. El espectro de la señal $m_i(t)$ se desplaza hasta quedar centrado en f_i. Para que este esquema funcione adecuadamente, f_i se debe elegir de modo que los anchos de banda de las distintas señales no se solapen de forma significativa. En caso contrario, resultaría imposible recuperar las señales originales.

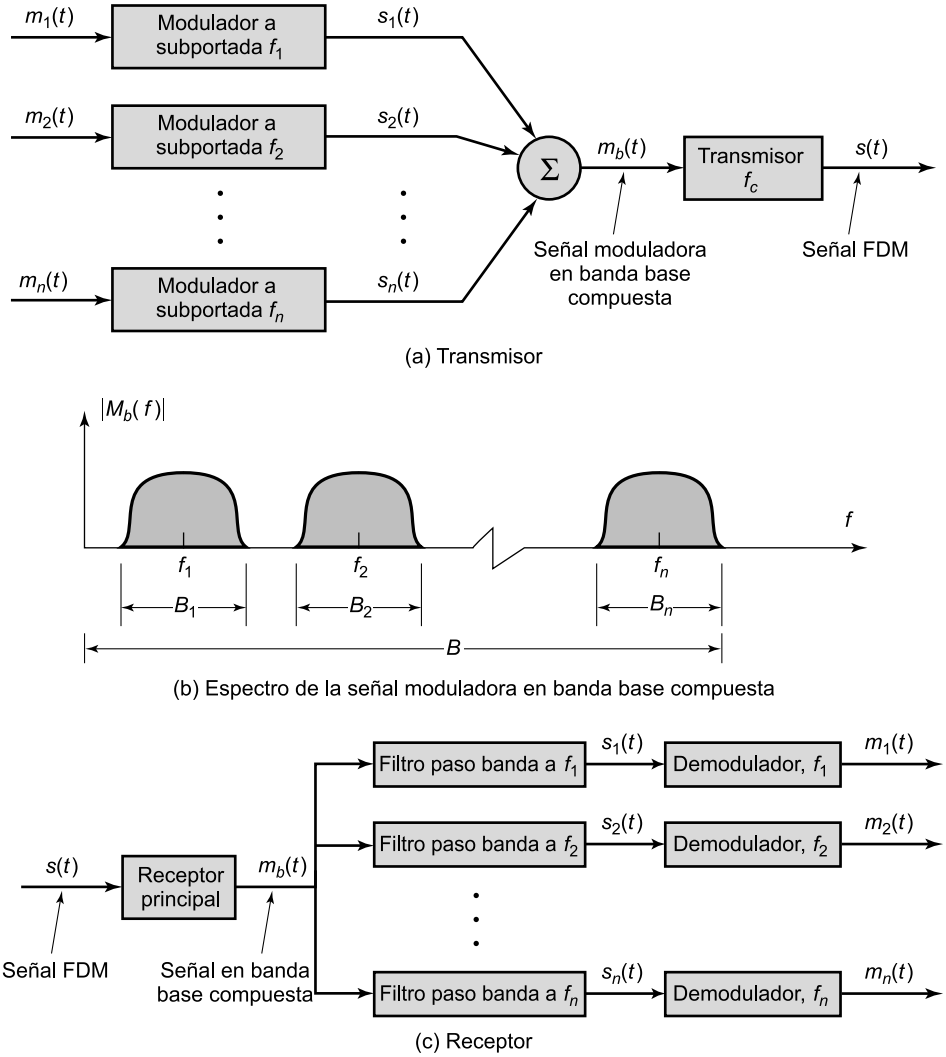


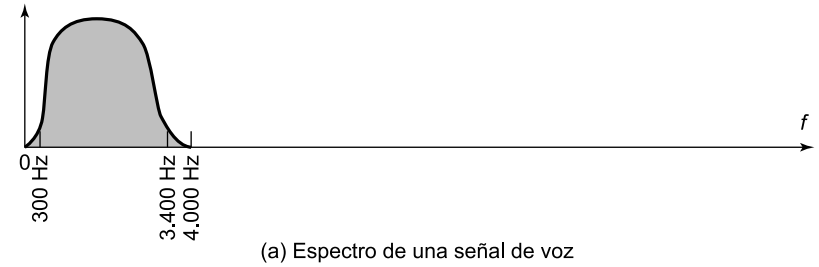
Figura 8.4. Sistema FDM [COUC01].

[1] El término *banda base* se emplea para designar la banda de frecuencias de la señal transmitida por la fuente y potencialmente usada como señal moduladora. Generalmente, el espectro de una señal en banda base es significativo en una banda que incluye o está en la vecindad de $f = 0$.

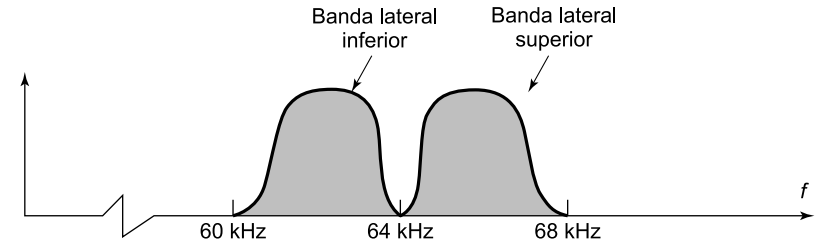
Tras esto, la señal compuesta puede desplazarse como un todo a otra frecuencia portadora a través de un proceso de modulación adicional. Posteriormente se verán ejemplos de esto. Este segundo paso de modulación no requiere hacer uso de la misma técnica de modulación que en el primero.

La señal FDM $s(t)$ tiene un ancho de banda total B, donde $B > \sum_{i=1}^{n} B_i$. Esta señal analógica se puede transmitir a través de un medio adecuado. En el extremo receptor se demodula la señal FDM para recuperar $m_b(t)$, la cual se hace pasar a través de n filtros paso banda, cada uno centrado en torno a f_i con un ancho de banda B_i, para $1 \leqslant i \leqslant n$. De esta forma, la señal se divide de nuevo en sus componentes, siendo cada una de ellas demodulada para recuperar la señal original correspondiente.

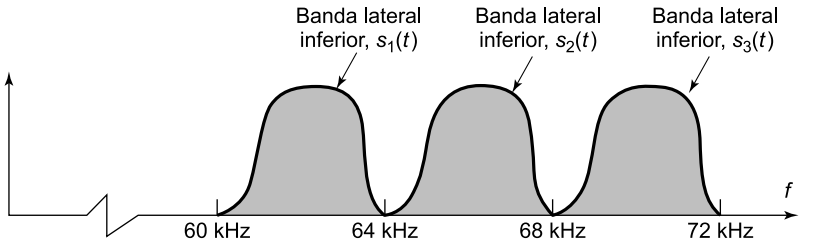
Ejemplo 8.2. Considérese un ejemplo sencillo consistente en la transmisión simultánea de tres señales de voz a través de un medio. Como se ha mencionado, el ancho de banda de una señal de voz se considera generalmente igual a 4 kHz, con un espectro efectivo comprendido entre los 300 y los 3.400 Hz (*véase* Figura 8.5a). Si una señal de este tipo se usa para modular en amplitud una portadora de 64 kHz, se obtiene el espectro de la Figura 8.5b. La señal modulada tiene un ancho de banda de 8 kHz, extendiéndose desde los 60 hasta los 68 kHz. Para hacer



(a) Espectro de una señal de voz



(b) Espectro de una señal de voz modulada a 64 kHz



(c) Espectro de la señal compuesta usando subportadoras de 64 kHz, 68 kHz y 72 kHZ

Figura 8.5. FDM de tres señales en la banda de voz.

un uso eficiente del ancho de banda, elegimos transmitir sólo la banda lateral inferior. Si se usan tres señales de voz para modular portadoras a frecuencias de 64, 68 y 72 kHz, y sólo se utiliza la banda lateral inferior de cada una de ellas, se obtiene el espectro de la Figura 8.5c.

Esta figura pone de manifiesto dos problemas con los que se enfrenta un sistema FDM. El primero es la diafonía, que puede aparecer si los espectros de señales componentes adyacentes se solapan de forma importante. En el caso de señales de voz, con un ancho de banda efectivo de sólo 3.100 Hz (de 300 a 3.400), resulta adecuado un ancho de banda de 4 kHz. El espectro de señales generadas por módems para transmisiones en la banda de voz también tiene buena cabida en este ancho de banda. Otro problema potencial es el ruido de intermodulación, estudiado en el Capítulo 3. En un enlace largo, los efectos no lineales de los amplificadores sobre una señal en un canal pueden dar lugar a componentes en frecuencia en otros canales.

SISTEMAS DE PORTADORA ANALÓGICA

El sistema de transmisión de larga distancia existente en los Estados Unidos y en todo el mundo ha sido diseñado para transmitir señales en la banda de voz a través de enlaces de transmisión de alta capacidad, como cable coaxial y sistemas de microondas. La primera técnica, y aún hoy de amplio uso, para la utilización de enlaces de alta capacidad es FDM. En los Estados Unidos, AT&T diseñó una jerarquía de esquemas FDM para dar cabida a sistemas de transmisión de distintas capacidades. Un sistema similar, aunque desafortunadamente distinto, fue adoptado internacionalmente bajo los auspicios de la ITU-T (*véase* Tabla 8.1).

Tabla 8.1. Estándares de portadora FDM norteamericanos e internacionales.

Número de canales de voz	Ancho de banda	Espectro	AT & T	ITU-T
12	48 kHz	60-108 kHz	Grupo	Grupo
60	240 kHz	312-552 kHz	Supergrupo	Supergrupo
300	1,232 MHz	812-2.044 kHz		Grupo maestro
600	2,52 MHz	564-3.084 kHz	Grupo maestro	
900	3,872 MHz	8,516-12,388 MHz		Grupo supermaestro
$N \times 600$			Grupo maestro multiplexado	
3.600	16,984 MHz	0,564-17,548 MHz	Grupo jumbo	
10.800	57,442 MHz	3,124-60,566 MHz	Grupo jumbo multiplexado	

En el primer nivel de la jerarquía AT&T se combinan 12 canales de voz para dar lugar a una señal grupo con un ancho de banda de 12×4 kHz = 48 kHz, en el rango 60-108 kHz. Las señales se generan de forma similar a la descrita previamente haciendo uso de frecuencias subportadoras

de entre 64 y 108 kHz en incrementos de 4 kHz. El siguiente bloque es el supergrupo de 60 canales, que está formado por cinco señales de grupo multiplexadas en frecuencia. En este nivel, cada grupo se trata como una única señal con un ancho de banda de 48 kHz, modulándose por la correspondiente subportadora. Las subportadoras tienen frecuencias comprendidas entre 420 y 612 kHz en incrementos de 48 kHz. La señal resultante ocupa la banda 312-552 kHz.

Existen distintas variantes para la formación de un supergrupo. Cada una de las cinco entradas al multiplexor de supergrupo puede ser un canal de grupo con 12 señales de voz multiplexadas. Es más, cualquier señal de hasta 48 kHz de ancho de banda contenida entre los 60 y los 108 kHz se puede usar como entrada al multiplexor de supergrupo. Otra posibilidad consiste en combinar 60 canales de ancho de banda de voz en un supergrupo, lo cual puede reducir los costes de multiplexación, ya que no se precisa una interfaz con el multiplexor de grupo.

El siguiente nivel de la jerarquía es el grupo maestro, en el que se combinan 10 supergrupos. Una vez más, cualquier señal con un ancho de banda de 240 kHz en el rango 312-552 kHz puede servir como entrada al multiplexor de grupo maestro. El grupo maestro tiene un ancho de banda de 2,52 MHz y puede soportar 600 canales de frecuencia de voz (VF, *Voice Frequency*). Como se muestra en la Tabla 8.1, por encima del grupo maestro se definen niveles de multiplexación superiores.

Obsérvese que la señal de voz o de datos original se puede modular varias veces. Por ejemplo, una señal de datos se puede codificar haciendo uso de QPSK para generar una señal de voz analógica. Esta señal se podría usar para modular una portadora de 76 kHz para producir una componente de una señal de grupo. Dicha señal de grupo puede usarse, a su vez, para modular una portadora de 516 kHz para dar lugar a una componente de una señal de supergrupo. Cada etapa puede distorsionar los datos originales; esto ocurre si, por ejemplo, el modulador/multiplexor presenta no linealidades o introduce ruido.

MULTIPLEXACIÓN POR DIVISIÓN EN LA LONGITUD DE ONDA

Toda la potencialidad de la fibra óptica puede explotarse mediante la transmisión de haces de luz a frecuencias diferentes sobre una misma fibra. Aunque esto es una forma de multiplexación por división en frecuencias (FDM), se denomina usualmente multiplexación por división en la longitud de onda (WDM, *Wavelength Division Multiplexing*). En WDM, el haz de luz a través de la fibra consta de varios colores, o longitudes de onda, cada uno de los cuales transporta un canal de datos distinto. En 1997 se alcanzó un hito cuando los Laboratorios Bell pusieron en marcha un sistema WDM con 100 haces, cada uno de ellos operando a 10 Gbps y consiguiéndose una velocidad total de 1 billón de bits por segundo (lo que se conoce como 1 terabit por segundo o 1 Tbps). En la actualidad existen sistemas comerciales con 160 canales de 10 Gbps. En entorno de laboratorio, Alcatel ha conseguido transportar 256 canales a 39,8 Gbps cada uno, lo que supone un total de 10,1 Tbps, sobre una distancia de 100 km.

Un sistema WDM típico tiene la misma arquitectura que uno FDM. Diversas fuentes generan un haz láser a diferentes longitudes de onda. Éstos son enviados a un multiplexor, el cual combina las fuentes para su transmisión sobre una misma línea de fibra. Amplificadores ópticos, generalmente espaciados decenas de kilómetros entre sí, se encargan de amplificar todas las longitudes de onda simultáneamente. Finalmente, la señal compuesta se recibe en el demultiplexor, donde se separan los canales componentes y se envían hacia los receptores pertinentes en el punto de destino.

La mayor parte de los sistemas WDM operan en el rango de 1.550 nm. En los primeros sistemas se reservaban 200 MHz para cada canal, pero en la actualidad la mayoría de los sistemas

WDM usan un espaciado de 50 GHz. El espaciado de canal definido en la norma G.692 de la ITU-T, que da cabida a 80 canales de 50 GHz, se resume en la Tabla 8.2.

Tabla 8.2. Espaciado entre canales en el sistema WDM de ITU-T (G.692).

Frecuencia (THz)	Longitud de onda en el vacío (nm)	50 GHz	100 GHz	200 GHz
196,10	1.528,77	X	X	X
196,05	1.529,16	X		
196,00	1.529,55	X	X	
195,95	1.529,94	X		
195,90	1.530,33	X	X	X
195,85	1.530,72	X		
195,80	1.531,12	X	X	
195,75	1.531,51	X		
195,70	1.531,90	X	X	X
195,65	1.532,29	X		
195,60	1.532,68	X	X	
…	…			
192,10	1.560,61	X	X	X

En la bibliografía puede encontrarse el término **multiplexación por división en la longitud de onda densa** (DWDM, *Dense WDM*). Aunque no existe una definición oficial o estándar del término, éste denota el empleo de más canales, más cercanos entre sí, que el WDM ordinario. En general, un espaciado de canal de 200 GHz o menos puede considerarse denso.

8.2. MULTIPLEXACIÓN POR DIVISIÓN EN EL TIEMPO SÍNCRONA

CARACTERÍSTICAS

La multiplexación por división en el tiempo síncrona es posible cuando la velocidad de transmisión alcanzable (a veces llamada inapropiadamente ancho de banda) por el medio excede la velocidad de las señales digitales a transmitir. Se pueden transmitir varias señales digitales (o señales analógicas que transportan datos digitales) a través de una única ruta de transmisión mediante la mezcla temporal de partes de cada una de las señales. El proceso de mezcla puede ser a nivel de bit o en bloques de octetos o cantidades superiores. Por ejemplo, consideremos que el multiplexor de la Figura 8.2b tiene seis entradas de, digamos, 9,6 kbps cada una. Una única línea con capacidad de, al menos, 57,6 kbps (más la capacidad suplementaria) puede dar cabida a las seis fuentes.

En la Figura 8.6 se muestra un esquema general de un sistema TDM síncrono. Se multiplexan varias señales $[m_i(t), i = 1, n]$ sobre el mismo medio de transmisión. Las señales transportan datos

digitales y son, en general, señales digitales. Los datos de entrada procedentes de cada fuente se almacenan brevemente en una memoria temporal o «buffer». Cada memoria temporal tiene una longitud típica de un bit o un carácter. Estas memorias temporales se sondean secuencialmente para componer una secuencia de datos digital compuesta, $m_c(t)$. El sondeo es lo suficientemente rápido para que cada memoria temporal se vacíe antes de que se reciban nuevos datos. Por tanto, la velocidad de $m_c(t)$ debe ser igual, al menos, a la suma de las velocidades de las señales $m_i(t)$. La señal digital $m_c(t)$ puede transmitirse directamente o se puede hacer pasar a través de un módem para dar lugar a una señal analógica. En ambos casos la transmisión es generalmente síncrona.

Los datos transmitidos pueden tener un formato similar al mostrado en la Figura 8.6b. Éstos se organizan en **tramas**, cada una de las cuales contiene un ciclo de ranuras temporales. En cada trama se dedican una o más ranuras a cada una de las fuentes de datos, denominándose **canal** a la secuencia de ranuras, de trama en trama, dedicadas a una fuente. La longitud de la ranura es igual a la longitud de la memoria temporal de transmisión, generalmente un bit o un carácter.

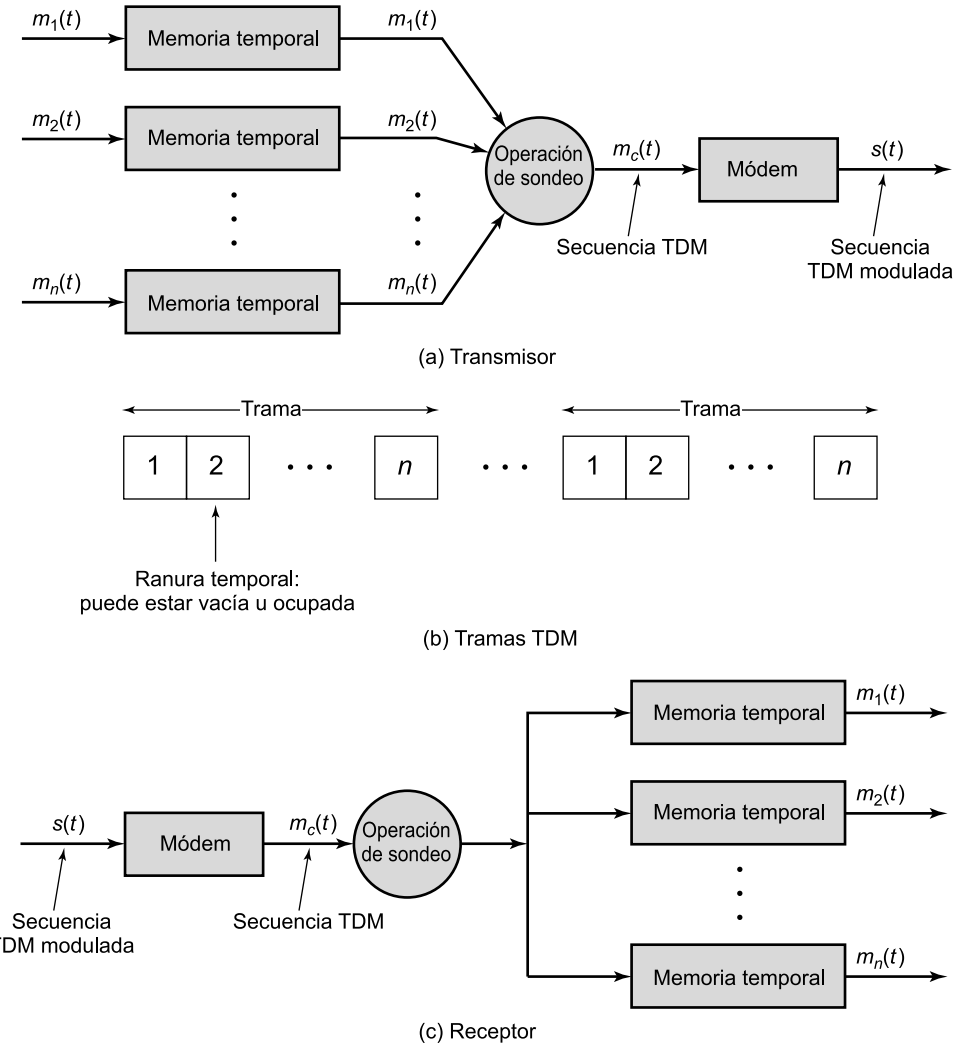


Figura 8.6. Sistema TDM síncrono.

La técnica de mezcla de caracteres se usa con fuentes síncronas y asíncronas, conteniendo cada ranura temporal un carácter de datos. Usualmente, los bits de principio y de fin de cada carácter se eliminan antes de la transmisión y se reinsertan por parte del receptor, mejorando así la eficiencia. La técnica de mezcla de bits se usa con fuentes síncronas, pudiendo utilizarse también con fuentes asíncronas. Cada ranura temporal contiene un único bit.

Los datos mezclados se demultiplexan en el receptor y se encaminan hacia la memoria temporal de destino apropiada. Para cada fuente de entrada $m_i(t)$ existe una fuente de salida idéntica que recibirá los datos de entrada a la misma velocidad a la que fueron generados.

La técnica TDM síncrona se denomina síncrona no porque se emplee transmisión síncrona, sino porque las ranuras temporales se preasignan y fijan a las distintas fuentes. Las ranuras temporales asociadas a cada fuente se transmiten tanto si éstas tienen datos que enviar como si no. Esto, por supuesto, también ocurre en FDM. En ambos casos se desaprovecha la capacidad a costa de simplificar la implementación. Sin embargo, un dispositivo TDM síncrono puede gestionar fuentes a distintas velocidades incluso cuando se hacen asignaciones fijas de las ranuras temporales. Por ejemplo, al dispositivo de entrada más lento se le podría asignar una ranura por ciclo, mientras que a los más rápidos se podrían asignar varias ranuras por ciclo.

CONTROL DEL ENLACE EN TDM

El lector habrá observado que la secuencia de datos transmitida mostrada en la Figura 8.6b no contiene las cabeceras y colas propias de la transmisión síncrona. La razón es que no son necesarios los mecanismos de control proporcionados por un protocolo de enlace de datos. Resulta instructivo hacer hincapié en este punto, para lo cual se considerarán dos mecanismos clave en el control del enlace de datos: control de flujo y control de errores. Es claro que el control de flujo no es necesario por lo que se refiere al multiplexor y al demultiplexor (*véase* Figura 8.1). La velocidad de datos es fija en la línea del multiplexor, estando éste y el demultiplexor diseñados para operar a esta velocidad. Pero supóngase que una de las líneas de salida está conectada a un dispositivo que es incapaz de aceptar datos temporalmente. ¿Debería cesar la transmisión de tramas TDM? Concluyentemente no, ya que las restantes líneas de salida están esperando a recibir datos en instantes de tiempo predeterminados. La solución consiste en que el dispositivo de salida que se ha saturado detenga el flujo de datos proveniente del correspondiente dispositivo de entrada. Así, el canal en cuestión transmitirá ranuras vacías durante algún tiempo, pero las tramas en su conjunto mantendrán la misma velocidad de transmisión.

El razonamiento es el mismo para el control de errores. No se debería solicitar la retransmisión de una trama TDM completa si ocurriera un error en uno de los canales. Los dispositivos que utilizan los otros canales no querrían una retransmisión ni sabrían que algún otro dispositivo en otro canal la ha solicitado. De nuevo, la solución consiste en aplicar el control de errores para cada canal de forma independiente.

El control de flujo y el control de errores pueden aplicarse para cada canal independientemente usando un protocolo de control del enlace de datos como HDLC. En la Figura 8.7 se muestra un ejemplo simplificado. Se suponen dos fuentes de datos, cada una de las cuales utiliza HDLC. Una de ellas transmite una secuencia de tramas HDLC de tres octetos de datos cada una, y la otra fuente transmite tramas HDLC con cuatro octetos de datos. Por sencillez, y aunque es más frecuente la mezcla de bits, supóngase que se usa multiplexación por mezcla de caracteres. Obsérvese lo que sucede. Los octetos de las tramas HDLC de las dos fuentes se transmiten juntos a través de la línea multiplexada. Al lector puede resultarle este diagrama inadecuado en principio, puesto que en cier-

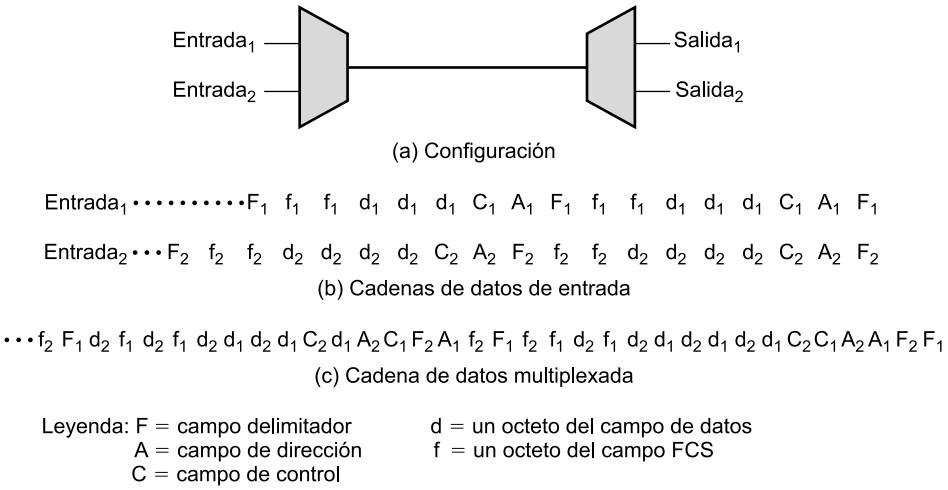

Entrada1
Entrada2
Salida1
Salida2
(a) Configuración
Entrada1 • • • • • • • • • • F1 f1 f1 d1 d1 d1 C1 A1 F1 f1 f1 d1 d1 d1 C1 A1 F1
Entrada2 • • • F2 f2 f2 d2 d2 d2 d2 C2 A2 F2 f2 f2 d2 d2 d2 d2 C2 A2 F2
(b) Cadenas de datos de entrada
• • • f2 F1 d2 f1 d2 f1 d2 d1 d2 d1 C2 d1 A2 C1 F2 A1 f2 F1 f2 f1 d2 f1 d2 d1 d2 d1 d2 d1 C2 C1 A2 A1 F2 F1
(c) Cadena de datos multiplexada
Leyenda: F = campo delimitador
A = campo de dirección
C = campo de control
d = un octeto del campo de datos
f = un octeto del campo FCS

Figura 8.7. Uso del control del enlace de datos en canales TDM.

to sentido las tramas HDLC han perdido su integridad. Por ejemplo, cada secuencia de comprobación de trama (FCS) en la línea se aplica a un conjunto distinto de bits. Incluso la FCS está dividida. No obstante, todas las piezas se ensamblan correctamente antes de que se reciban en el dispositivo correspondiente al otro extremo del protocolo HDLC. En este sentido, la operación de multiplexación/demultiplexación es transparente para las estaciones conectadas; es como si existiese un enlace dedicado para cada par de estaciones comunicadas.

En la Figura 8.7 se necesita una mejora. Ambos extremos de la línea tienen que ser una combinación multiplexor/demultiplexor con una línea *full-duplex* entre ellos. Así pues, cada canal consta de dos conjuntos de ranuras, una en cada sentido de la transmisión. Los dispositivos individuales conectados en cada extremo pueden, en parejas, usar HDLC para controlar su propio canal. Los multiplexores/demultiplexores no necesitan preocuparse de estas cuestiones.

Delimitación de tramas

Ya se ha visto que no es preciso un protocolo de control del enlace para gestionar la línea TDM. No obstante, es necesaria una delimitación básica. Dado que no se han especificado indicadores o caracteres SYNC para delimitar las tramas TDM, es necesario algún método para asegurar la sincronización de éstas. Es clara la importancia de mantener la sincronización de trama, ya que si la fuente y el destino se desincronizasen se perderían los datos de todos los canales.

Quizá, el mecanismo más usual para llevar a cabo la delimitación de tramas sea el conocido como delimitación por dígitos añadidos. Generalmente, en este esquema se incluye un bit de control en cada trama TDM. A modo de «canal de control», en cada trama se usa una combinación predefinida de bits. Un ejemplo típico es el patrón de bits alternantes 101010..., cuya aparición resulta poco probable en un canal de datos. De este modo, para sincronizar, el receptor compara los bits de entrada en una determinada posición de la trama con el patrón esperado. Si no coinciden, se compara con los bits sucesivos hasta que se encuentre la combinación de bits y el patrón persista a lo largo de varias tramas. Una vez realizada la sincronización, el receptor continúa la monitorización del canal de bits de delimitación. Si desaparece el patrón, el receptor debe llevar a cabo de nuevo el proceso de búsqueda.

Inserción de bits

Quizá, el problema más difícil en el diseño de un multiplexor por división en el tiempo síncrono sea el relativo a la sincronización de las distintas fuentes de datos. Si cada fuente dispone de un reloj independiente, cualquier variación entre los relojes puede causar la pérdida del sincronismo. En algunos casos puede suceder también que las velocidades de datos de las secuencias de entrada no estén relacionadas por un número racional simple. En ambos casos resulta efectivo el uso de la técnica conocida como inserción de bits. En ella, la velocidad de salida del multiplexor, excluyendo los bits de delimitación, es mayor que la suma de las velocidades de entrada instantáneas máximas. La capacidad extra se emplea en la inclusión de pulsos o bits adicionales sin significado en cada señal de entrada hasta que su velocidad sea igual a la de una señal de reloj generada localmente. Los pulsos insertados lo son en posiciones fijas dentro del formato de trama del multiplexor, de manera que puedan ser identificados y eliminados en el demultiplexor.

Ejemplo 8.3. Un ejemplo, extraído de [COUC01], ilustra el uso de TDM síncrona para multiplexar fuentes analógicas y digitales (*véase* Figura 8.8). Considérese la existencia de 11 fuentes a multiplexar en un enlace:

Fuente 1: analógica, con 2 kHz de ancho de banda.

Fuente 2: analógica, con 4 kHz de ancho de banda.

Fuente 3: analógica, con 2 kHz de ancho de banda.

Fuentes 4-11: digitales síncronas a 7.200 bps.

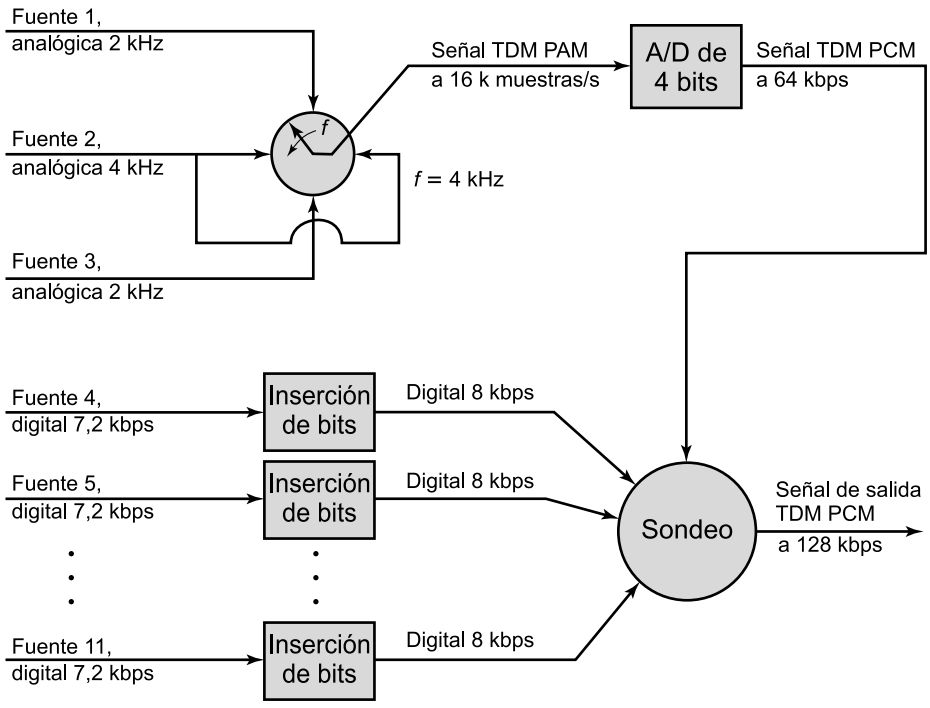


Figura 8.8. TDM para fuentes analógicas y digitales [COUC01].

En primer lugar, se convierten a digital las fuentes analógicas haciendo uso de la técnica PCM. Recuérdese del Capítulo 5 que PCM se fundamenta en el teorema de muestreo, el cual establece que una señal se debe muestrear a una velocidad igual a dos veces su ancho de banda. Por tanto, la velocidad de muestreo para las fuentes 1 y 3 será de 4.000 muestras por segundo, y de 8.000 muestras por segundo para la fuente 2. Estas muestras, de naturaleza analógica (PAM), se deben cuantificar o digitalizar. Supóngase que se usan 4 bits para cada muestra analógica. Por comodidad, estas tres fuentes se multiplexarán en primer lugar, como una sola. A una velocidad de sondeo de 4 kHz, se toma por cada ciclo una muestra PAM de las fuentes 1 y 3 de forma alternativa, y dos muestras PAM de la fuente 2. Estas cuatro muestras se mezclan y convierten a muestras PCM de 4 bits. Se genera así un total de 16 bits a razón de 4.000 veces por segundo, dando lugar a una velocidad compuesta de 64 kbps.

Para las fuentes digitales se usa inserción de bits con objeto de que cada fuente alcance una velocidad de 8 kbps, para una velocidad conjunta de 64 kbps. Una trama puede constar de varios ciclos de 32 bits, disponiendo cada uno de ellos de 16 bits PCM y dos bits para cada una de las ocho fuentes digitales.

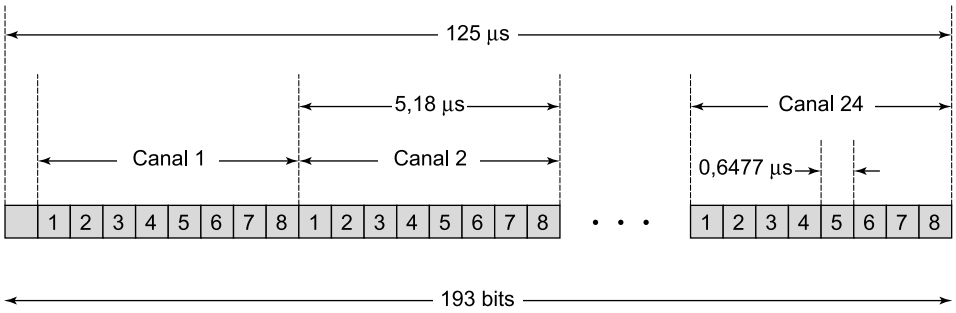
SISTEMAS DE PORTADORA DIGITAL

El sistema de transmisión de larga distancia de los Estados Unidos y del resto del mundo se diseñó para transmitir señales de voz a través de enlaces de transmisión de alta capacidad, como fibra óptica, cable coaxial y microondas. Parte de la evolución de estas redes de telecomunicación hacia la tecnología digital ha consistido en la adopción de estructuras de transmisión TDM síncrona. En los Estados Unidos, AT&T desarrolló una jerarquía de estructuras TDM con diferentes capacidades; esta estructura se ha adoptado también en Canadá y en Japón. Una jerarquía análoga, aunque por desgracia no idéntica, ha sido adoptada internacionalmente bajo los auspicios de la ITU-T (*véase* Tabla 8.3).

Tabla 8.3. Estándares TDM norteamericanos e internacionales.

Norteamérica			Internacional (ITU-T)		
Nomenclatura	**Número de canales de voz**	**Velocidad (Mbps)**	**Nivel**	**Número de canales de voz**	**Velocidad (Mbps)**
DS-1	24	1,544	1	30	2,048
DS-1C	48	3,152	2	120	8,448
DS-2	96	6,312	3	480	34,368
DS-3	672	44,736	4	1.920	139,264
DS-4	4.032	274,176	5	7.680	565,148

La base de la jerarquía TDM (en Norteamérica y Japón) es el formato de transmisión DS-1 (*véase* Figura 8.9), en el que se multiplexan 24 canales. Cada trama contiene 8 bits por canal más un bit de delimitación; es decir, $24 \times 8 + 1 = 193$ bits. Para transmisiones de voz se aplican las siguientes reglas. Cada canal contiene una palabra de datos de voz digitalizada. La señal de voz analógica original se digitaliza haciendo uso de la técnica de modulación por codificación de pulso (PCM) a una velocidad de 8.000 muestras por segundo. Por tanto, cada canal, y en consecuencia cada trama, se debe repetir 8.000 veces por segundo. Con una trama de longitud de 193 bits se



Notas:
1. El primer bit es de delimitación, usado para sincronización.
2. Canales de voz:
   - PCM 8 bit usado en cinco de cada seis tramas.
   - PCM 7 bit usado en una de cada seis tramas; el bit 8 de cada canal es de señalización.
3. Canales de datos:
   - El canal 24 se emplea para señalización sólo en algunos esquemas.
   - Los bits del 1 al 7 se usan para el servicio a 56 kbps.
   - Los bits 2-7 se usan para servicios a 9,6 kbps, 4,8 kbps y 2,4 kbps.

Figura 8.9. Formato de transmisión DS-1.

dispone, pues, de una velocidad de $8.000 \times 193 = 1{,}544$ Mbps. En cinco de cada seis tramas se utilizan muestras PCM de 8 bits. Cada seis tramas, cada uno de los canales contiene una palabra PCM de 7 bits más un *bit de señalización*. Los bits de señalización forman una secuencia para cada canal de voz que contiene información de control de red y de encaminamiento. Por ejemplo, las señales de control se emplean para establecer una conexión o para finalizar una llamada.

El formato DS-1 se emplea también para proporcionar servicio de datos digitales. Por cuestiones de compatibilidad con la voz, se usa la misma velocidad de 1,544 Mbps. En este caso existen 23 canales de datos. El canal de posición vigésimo cuarta se reserva para un carácter especial *sync*, que permite una recuperación más rápida y fiable de la delimitación tras un error en la misma. En cada canal se usan 7 bits de datos por trama, indicando el octavo bit si el canal, en esa trama, contiene datos de usuario o de control del sistema. Con 7 bits por canal, y dado que cada trama se repite 8.000 veces por segundo, se obtiene una velocidad de datos por canal de 56 kbps. Se pueden conseguir velocidades inferiores a través de la utilización de una técnica conocida como multiplexación de baja velocidad. En esta técnica se dedica un bit adicional de cada canal para indicar qué velocidad se va a proporcionar. Esto da una capacidad total por canal de $6 \times 8.000 = 48$ kbps. Esta capacidad se utiliza para multiplexar cinco canales a 9,6 kbps, diez canales a 4,8 kbps o veinte canales a 2,4 kbps. Por ejemplo, si se usa el canal 2 para proporcionar un servicio a 9,6 kbps, hasta cinco subcanales de datos compartirán entonces este subcanal. Los datos de cada subcanal aparecen como seis bits en el canal 2 cada cinco tramas.

Finalmente, el formato DS-1 se puede usar también para transportar una mezcla de canales de voz y de datos. En este caso se utilizan los 24 canales, no existiendo octeto *sync*.

Por encima de la velocidad de 1,544 Mbps proporcionada por DS-1, se obtienen niveles superiores de multiplexación mediante la mezcla de bits procedentes de entradas DS-1. Por ejemplo, el sistema de transmisión DS-2 combina cuatro entradas DS-1 en una cadena de 6,312 Mbps. Los datos de las cuatro fuentes se mezclan a razón de 12 bits cada vez. Obsérvese que $1{,}544 \times 4 = 6{,}176$ Mbps; la capacidad restante se emplea para bits de delimitación y de control.

SONET/SDH

La Red Óptica Síncrona (SONET, *Synchronous Optical NETwork*) es una interfaz de transmisión óptica propuesta originalmente por BellCore y normalizada por ANSI. La ITU-T ha publicado, en la recomendación G.707[2], una versión compatible denominada Jerarquía Digital Síncrona (SDH, *Synchronous Digital Hierarchy*). SONET se ideó para proporcionar una especificación que aproveche las ventajas que proporciona la transmisión digital de alta velocidad a través de fibra óptica.

Jerarquía de señal

La especificación SONET define una jerarquía de velocidades de datos digitales normalizadas (*véase* Tabla 8.4). En el nivel más bajo, denominado STS-1 (*Synchronous Transport Signal level 1*) u OC-1 (*Optical Carrier level 1*)[3], la velocidad es 51,84 Mbps. Esta velocidad se puede usar para transportar una sola señal DS-3 o un grupo de señales a velocidad inferior, como DS1, DS1C, DS2 y otras velocidades ITU-T (por ejemplo, 2,048 Mbps).

Se pueden combinar varias señales STS-1 para formar una señal STS-N. La señal se crea mezclando octetos de *N* señales STS-1 mutuamente sincronizadas.

La velocidad menor considerada en la jerarquía digital síncrona de la ITU-T es 155,52 Mbps, denominada STM-1. Ésta se corresponde con STS-3 de SONET.

Tabla 8.4. Jerarquía de señal en SONET/SDH.

Nomenclatura SONET	Nomenclatura ITU-T	Velocidad	Velocidad de información útil (Mbps)
STS-1/OC-1	STM-0	51,84 Mbps	50,112 Mbps
STS-3/OC-3	STM-1	155,52 Mbps	150,336 Mbps
STS-9/OC-9		466,56 Mbps	451,008 Mbps
STS-12/OC-12	STM-4	622,08 Mbps	601,344 Mbps
STS-18/OC-18		933,12 Mbps	902,016 Mbps
STS-24/OC-24		1,24416 Gbps	1,202688 Gbps
STS-36/OC-36		1,86624 Gbps	1,804032 Gbps
STS-48/OC-48	STM-16	2,48832 Gbps	2,405376 Gbps
STS-96/OC-96		4,87664 Gbps	4,810752 Gbps
STS-192/OC-192	STM-64	9,95328 Gbps	9,621504 Gbps
STS-768	STM-256	39,81312 Gbps	38,486016 Gbps
STS-3072		159,25248 Gbps	1,53944064 Gbps

Formato de trama

El bloque básico en SONET es la trama STS-1, que consta de 810 octetos y se transmite a razón de una cada 125 μs, dando lugar a una velocidad total de 51,84 Mbps (*véase* Figura 8.10a). La trama se puede ver desde un punto de vista lógico como una matriz de 9 filas de 90 octetos cada una, transmitiéndose por filas de izquierda a derecha y de arriba abajo.

---

[2] En adelante usaremos el término *SONET* para referirnos a ambas especificaciones, señalándose explícitamente las diferencias cuando éstas existan.

[3] Una velocidad OC-*N* es la equivalente a una señal eléctrica STS-*N*. Los dispositivos de usuario finales transmiten y reciben señales eléctricas, las cuales deben convertirse a y desde señales ópticas para su transmisión a través de fibras ópticas.

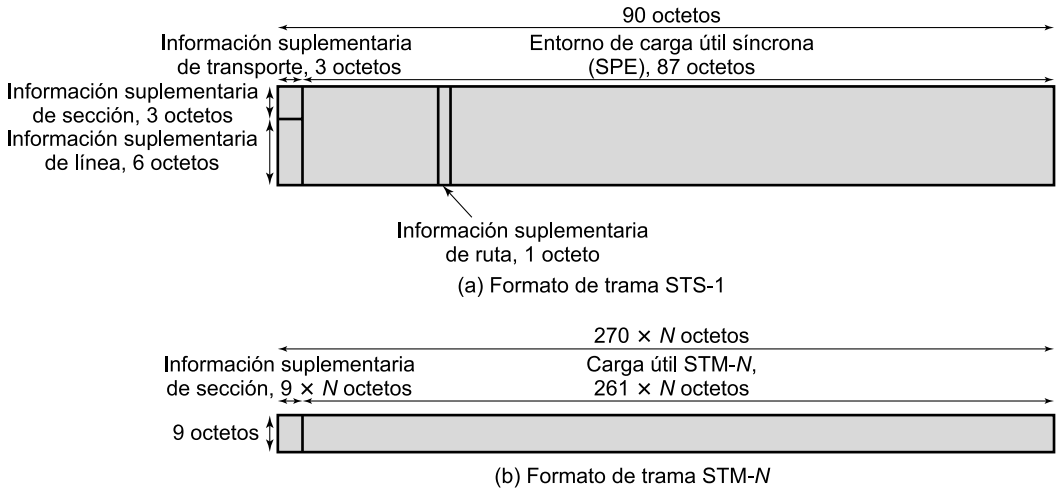

90 octetos
Información suplementaria de transporte, 3 octetos
Entorno de carga útil síncrona (SPE), 87 octetos
Información suplementaria de sección, 3 octetos
Información suplementaria de línea, 6 octetos
Información suplementaria de ruta, 1 octeto
(a) Formato de trama STS-1
270 × N octetos
Información suplementaria de sección, 9 × N octetos
Carga útil STM-N, 261 × N octetos
9 octetos
(b) Formato de trama STM-N

Figura 8.10. Formatos de trama SONET/SDH.

Las tres primeras columnas (3 octetos × 9 filas = 27 octetos) de la trama son octetos suplementarios. Nueve de ellos están dedicados a información suplementaria relacionada con las secciones y los otros 18 se dedican a información suplementaria de línea. En la Figura 8.11a se muestra la disposición de los octetos suplementarios, definiéndose los distintos campos en la Tabla 8.5.

El resto de la trama es información útil, también denomina carga útil o *payload*. Ésta incluye una columna de información suplementaria relacionada con la ruta, que no ocupa necesariamente la primera columna disponible; la información suplementaria de línea contiene un puntero que indica dónde comienza la información suplementaria de ruta. En la Figura 8.11b se muestra la disposición de los octetos suplementarios de ruta, definiéndose éstos en la Tabla 8.5.

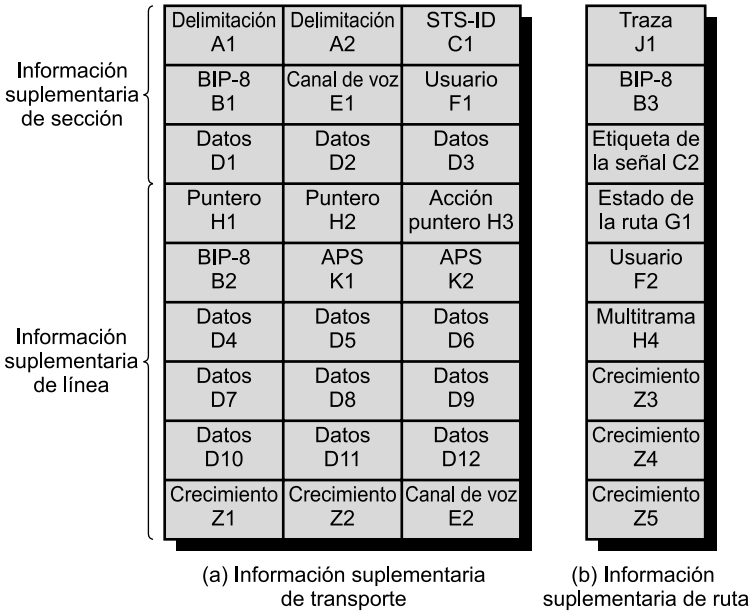


Figura 8.11. Octetos de información suplementaria en STS-1 de SONET.

La Figura 8.10b muestra el formato general para tramas de velocidad superior usando la nomenclatura de la ITU-T.

Tabla 8.5. Bits de información suplementaria en STS-1.

Información suplementaria de sección	
A1, A2:	Octetos de delimitación = F6,28 HEX; usados para sincronizar el comienzo de cada trama.
C1:	STS-1 ID identifica el número STS-1 (de 1 a N) para cada STS-1 en un multiplexor STS-N.
B1:	Octeto de paridad de la mezcla de bits (*bit-interleaved parity*); se usa paridad par sobre la trama STS-1 anterior tras la mezcla; el bit *i*-ésimo de este octeto contiene el resultado de una operación de paridad par entre los bits de posición *i*-ésima de todos los octetos de la trama previa.
E1:	Este octeto a nivel de sección proporciona 64 kbps PCM; canal de voz de 64 kbps opcional a usar entre equipos terminales, concentradores y terminales remotos.
F1:	Canal a 64 kbps independiente para necesidades de usuario.
D1-D3:	Canal de comunicaciones de datos a 192 kbps para alarmas, mantenimiento, control y administración entre secciones.
Información suplementaria de línea	
H1-H3:	Octetos de puntero para el alineamiento de trama y ajuste de la frecuencia de los datos correspondientes a la carga útil.
B2:	Paridad de la mezcla de bits para monitorizar errores a nivel de línea.
K1, K2:	Dos octetos reservados para la señalización entre equipos de conmutación con protección automática a nivel de línea; se utiliza un protocolo orientado a bit que proporciona protección de errores y gestión del enlace óptico SONET.
D4-D12:	Canal de comunicaciones de datos a 576 kbps para alarmas, mantenimiento, control, monitorización y administración a nivel de línea.
Z1, Z2:	Reservados para uso futuro.
E2:	Canal de voz PCM a 64 kbps para nivel de línea.
Información suplementaria de ruta	
J1:	Canal a 64 kbps usado para enviar repetidamente una cadena de longitud fija de 64 octetos de modo que un terminal receptor pueda verificar continuamente la integridad de una ruta; el contenido del mensaje es programable por el usuario.
B3:	Paridad de mezcla de bits a nivel de ruta, calculada sobre todos los bits del SPE previo.
C2:	Etiqueta de la señal de ruta STS que se utiliza para distinguir entre señales equipadas y no equipadas. *No equipadas* significa que la conexión de línea está completa pero no existen datos acerca de la ruta para enviar. En las señales equipadas, la etiqueta puede indicar una correspondencia específica para la información útil STS, necesaria para que los terminales receptores la interpreten correctamente.
G1:	Octeto de estado enviado desde el equipo de destino de la ruta al equipo origen de la misma para comunicar su estado así como las prestaciones de los errores en la ruta.
F2:	Canal de 64 kbps para el usuario de la ruta.
H4:	Indicador de multitrama para cargas útiles que requieran tramas de mayor longitud que una sola STS; los indicadores de multitrama se emplean cuando se empaquetan canales a velocidades inferiores (afluentes virtuales) en el SPE.
Z3-Z5:	Reservados para usos futuros.

8.3. MULTIPLEXACIÓN POR DIVISIÓN EN EL TIEMPO ESTADÍSTICA

CARACTERÍSTICAS

En un multiplexor por división en el tiempo síncrona es usual que se desaprovechen muchas de las ranuras temporales dentro de una trama. Una aplicación típica de TDM síncrona es la conexión de varios terminales a un puerto de computador compartido. Incluso en el caso de que todos los terminales se estén utilizando activamente, la mayor parte del tiempo no existe transferencia de datos en ningún terminal.

Una alternativa a la técnica TDM síncrona es la TDM estadística. El multiplexor estadístico explota esta propiedad usual en la transmisión de datos mediante la reserva dinámica bajo demanda de las ranuras o divisiones temporales. Al igual que en TDM síncrona, el multiplexor estadístico tiene varias líneas de entrada/salida por un lado y una línea multiplexada de velocidad superior por otro. Cada línea de entrada/salida tiene asociada una memoria temporal. En el caso del multiplexor estadístico hay n líneas de entrada/salida, pero sólo k, con $k < n$, ranuras temporales disponibles en cada trama TDM. La función de entrada del multiplexor consiste en sondear las memorias de almacenamiento de entrada para la captura de datos hasta que se complete una trama, enviando ésta posteriormente. Por lo que se refiere a la función de salida, el multiplexor recibe la trama y distribuye las ranuras temporales de datos a las memorias temporales de salida correspondientes.

Dado que en la técnica TDM estadística los dispositivos conectados no transmiten durante todo el tiempo, la velocidad de la línea multiplexada es menor que la suma de las velocidades de los dispositivos conectados. Así, un multiplexor estadístico puede usar una velocidad inferior para dar servicio a un número de dispositivos igual al soportado por un multiplexor síncrono. O dicho de otra forma, si un multiplexor estadístico y uno síncrono usan un enlace de la misma velocidad, el multiplexor estadístico puede dar servicio a más dispositivos.

En la Figura 8.12 se comparan las técnicas TDM síncrona y estadística. En la figura se consideran cuatro fuentes de datos y se muestran los datos generados en cuatro intervalos de tiempo (t_0, t_1, t_2, t_3). En el caso del multiplexor síncrono se tiene una velocidad de salida efectiva de cuatro

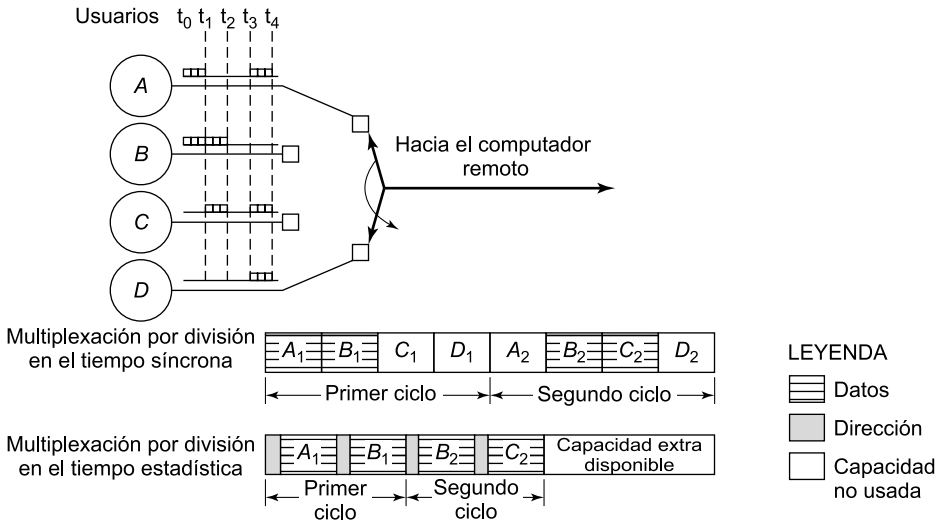


Figura 8.12. Comparación de las técnicas TDM síncrona y estadística.

veces la velocidad de cualquiera de los dispositivos de entrada. Durante cada intervalo, los datos se toman de las cuatro fuentes y posteriormente se envían. Por ejemplo, en el primer intervalo las fuentes C y D no producen datos, de modo que dos de las cuatro ranuras temporales transmitidas por el multiplexor se encuentran vacías.

Por el contrario, el multiplexor estadístico no envía ranuras temporales vacías mientras haya datos que enviar. Así, durante el primer intervalo sólo se envían las ranuras de A y B. Ahora bien, con este esquema se pierde el significado posicional de las ranuras; es decir, no se sabe a priori qué fuente de datos utilizará cada ranura. Así pues, dado que los datos se reciben desde y se distribuyen hacia las líneas de entrada/salida de forma impredecible, se precisa información de direccionamiento para asegurar que el envío se realiza de forma apropiada. Por tanto, en el caso de la técnica TDM estadística existe más información suplementaria por ranura, ya que cada una de ellas transporta una dirección además de los datos propiamente dichos.

La estructura de trama usada por un multiplexor estadístico repercute en las prestaciones finales del mismo. Es claro que resulta deseable minimizar la cantidad de bits suplementarios, con objeto de mejorar la eficiencia. En general, un sistema TDM estadístico usa un protocolo síncrono, como HDLC. Dentro de una trama HDLC, la trama de datos debe contener bits de control para el proceso de multiplexación. En la Figura 8.13 se muestran dos formatos posibles. En el primer caso sólo se incluye una fuente de datos por trama. Esta fuente se identifica mediante una dirección. La longitud del campo de datos es variable, quedando marcado su final por el final de toda la trama. Este esquema puede funcionar adecuadamente para baja carga, pero resulta bastante ineficiente en condiciones de alta carga.

Una forma de mejorar la eficiencia consiste en permitir que se empaqueten varias fuentes de datos en una misma trama. En este caso es necesario, sin embargo, algún procedimiento para especificar la longitud de los datos de cada una de las fuentes. De este modo, la subtrama TDM estadística consta de una secuencia de campos de datos, cada uno de ellos etiquetado con una dirección y una longitud. Pueden usarse diversas técnicas para hacer aún más eficiente esta aproximación. El campo de dirección se puede reducir a través del uso de direcciones relativas; es decir, cada dirección especifica el número de la fuente actual relativa a la anterior, módulo el número total de fuentes. Así, por ejemplo, en lugar de un campo de dirección de 8 bits, bastaría con uno de 4 bits.

Otra mejora posible es el uso de una etiqueta de dos bits con el campo de longitud. Un valor de 00, 01 o 10 corresponde con un campo de datos de uno, dos o tres octetos, no siendo necesario considerar un campo de longitud. Un valor 11 indicaría que se incluye el campo de longitud.

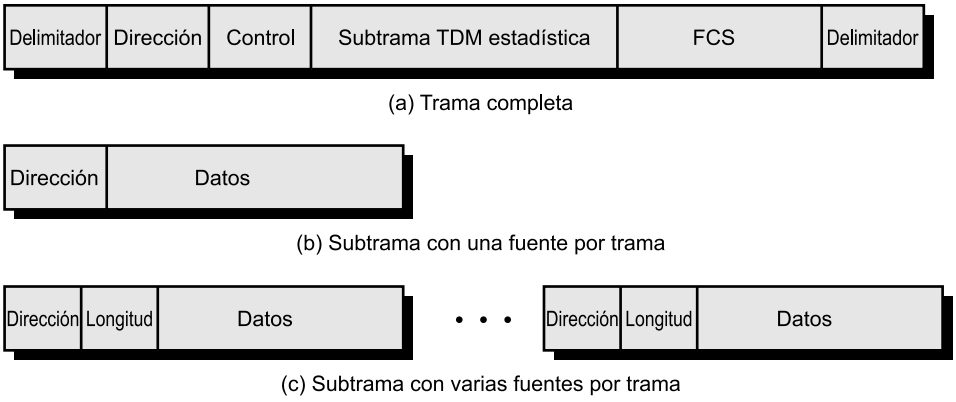


Figura 8.13. Tamaño de la memoria temporal y retardo para un multiplexor estadístico.

Otra posibilidad consiste en multiplexar en una sola trama de datos un carácter de cada una de las fuentes de datos que tienen un carácter que enviar. En este caso, la trama comienza con una secuencia de bits de indicación de longitud igual al número de fuentes, de forma que cuando una fuente dispone de un carácter para enviar durante una trama dada, activa el bit correspondiente.

PRESTACIONES

Ya se ha mencionado que la velocidad de salida de un multiplexor estadístico es menor que la suma de las velocidades de las entradas. Esto está permitido puesto que se supone que la cantidad media de datos de entrada es menor que la capacidad de la línea multiplexada. El problema de este esquema es que, aunque la entrada conjunta promedio puede ser menor que la capacidad de la línea multiplexada, puede haber periodos de pico en los que la entrada exceda la capacidad.

La solución a este problema consiste en incluir una memoria temporal en el multiplexor para almacenar temporalmente el exceso de datos de entrada. En la Tabla 8.6 se muestra un ejemplo del comportamiento de este tipo de sistemas. Se suponen 10 fuentes, cada una de ellas con una capacidad de 1.000 bps, y que la entrada media por fuente es el 50% del máximo. Así, en promedio, la carga de entrada es 5.000 bps. Se consideran dos casos: multiplexores con capacidad de salida de 5.000 bps y de 7.000 bps. Las entradas en la tabla mencionada muestran el número de bits de entrada procedentes de cada uno de los 10 dispositivos por cada milisegundo y la salida del multiplexor. Cuando la entrada excede la salida, el exceso se debe almacenar temporalmente.

Existe un compromiso entre el tamaño de la memoria temporal usada y la velocidad de la línea. Sería deseable usar tanto la memoria como la velocidad menores posibles, pero una reducción en uno de estos parámetros requiere el incremento del otro. Téngase en cuenta que el deseo de reducir el tamaño de la memoria temporal no se debe al coste de ésta —la memoria es barata—, sino al hecho de que a más cantidad de memoria mayor es el retardo. Por tanto, el compromiso real está en la relación entre el tiempo de respuesta del sistema y la velocidad de la línea multiplexada. En esta sección se presentan algunas medidas aproximadas para evaluar este compromiso. Estas medidas son suficientes para la mayoría de las situaciones.

Definamos los siguientes parámetros para un multiplexor por división en el tiempo estadístico:

I = número de fuentes de entrada.

R = velocidad de cada fuente, en bps.

M = capacidad efectiva de la línea multiplexada, en bps.

α = fracción media de tiempo que transmite cada fuente, $0 < \alpha < 1$.

$K = \dfrac{M}{IR}$ = razón entre la capacidad de la línea multiplexada y la entrada máxima total.

El parámetro M se ha definido teniendo en consideración los bits suplementarios incluidos por el mutiplexor; es decir, M representa la velocidad máxima a la que se pueden transmitir los bits de datos.

El parámetro K es una medida de la compresión alcanzada por el multiplexor. Por ejemplo, para una capacidad M dada, si $K = 0{,}25$ se gestionan, utilizando la misma capacidad de enlace, cuatro veces más dispositivos que mediante un multiplexor por división en el tiempo síncrona. El valor de K se puede acotar por:

$$\alpha < K < 1$$

Tabla 8.6. Ejemplo de las prestaciones de un multiplexor estadístico.

	Capacidad = 5.000 bps		Capacidad = 7.000 bps	
Entrada[a]	Salida	Exceso	Salida	Exceso
6	5	1	6	0
9	5	5	7	2
3	5	3	5	0
7	5	5	7	0
2	5	2	2	0
2	4	0	2	0
2	2	0	2	0
3	3	0	3	0
4	4	0	4	0
6	5	1	6	0
1	2	0	1	0
10	5	5	7	3
7	5	7	7	3
5	5	7	7	1
8	5	10	7	2
3	5	8	5	0
6	5	9	6	0
2	5	6	2	0
9	5	10	7	2
5	5	10	7	0

[a] Entrada = 10 fuentes, 1.000 bps/fuente; velocidad de entrada promedio = 50 % del máximo.

Un valor de $K = 1$ corresponde a un multiplexor por división en el tiempo síncrono, ya que el sistema tiene capacidad para servir todos los dispositivos de entrada al mismo tiempo. Si $K < \alpha$, la entrada excederá la capacidad del multiplexor.

Se pueden obtener algunos resultados considerando al multiplexor como una cola atendida por un solo servidor. Se alcanza una situación de cola cuando un servicio recibe un «cliente» y, al encontrarlo ocupado, tiene que esperar. El retardo sufrido por un cliente es el tiempo de espera en la cola más el tiempo de servicio. El retardo depende del patrón de tráfico de llegada y de las características del servidor. En la Tabla 8.7 se resumen los resultados para una distribución de llegadas aleatorias (Poisson) y un tiempo de servicio constante. Este modelo se puede relacionar fácilmente con el multiplexor estadístico:

$$\lambda = \alpha IR \qquad T_s = \frac{1}{M}$$

Tabla 8.7. Colas de un único servidor con tiempos de servicio constantes y distribución de llegadas de tipo Poisson (aleatorias).

Parámetros
λ = número medio de llegadas por segundo T_s = tiempo de servicio para cada llegada ρ = utilización; fracción de tiempo que está ocupado el servidor N = número medio de «clientes» en el sistema (en espera y siendo servidos) T_r = tiempo de estancia; tiempo medio que un «cliente» pasa en el sistema (en espera y siendo servido) σ_r = desviación estándar de T_r
Fórmulas
$\rho = \lambda T_s$ $N = \frac{\rho^2}{2(1-\rho)} + \rho$ $T_r = \frac{T_s(2-\rho)}{2(1-\rho)}$ $\sigma_r = \frac{1}{1-\rho}\sqrt{\rho - \frac{3\rho^2}{2} + \frac{5\rho^3}{6} - \frac{\rho^4}{12}}$

La velocidad de llegada promedio λ, en bps, es igual a la entrada potencial total (IR) multiplicada por la fracción de tiempo α con que transmite cada fuente. El tiempo de servicio T_s, en segundos, es el tiempo empleado en transmitir un bit, que es $1/M$, Obsérvese que

$$\rho = \lambda T_s = \frac{\alpha IR}{M} = \frac{\alpha}{K} = \frac{\lambda}{M}$$

El parámetro ρ es la utilización o fracción de la capacidad total del enlace utilizada. Por ejemplo, si la capacidad M es 50 kbps y $\rho = 0{,}5$, la carga del sistema es 25 kbps. El parámetro N en la Tabla 8.7 es una medida de la capacidad de memoria temporal utilizada en el multiplexor. Por último, T_r es una medida del retardo promedio sufrido por una fuente de entrada.

La Figura 8.14 puede aclarar conceptualmente el compromiso entre el tiempo de respuesta del sistema y la velocidad de la línea multiplexada. Se supone que los datos se transmiten en tramas de 1.000 bits. En la parte (a) de la figura mencionada se representa el número medio de tramas que deben almacenarse temporalmente en función de la utilización media de la línea multiplexada; utilización que se expresa como un porcentaje de la capacidad total de la línea. Así, si la carga de entrada media es 5.000 bps, la utilización es del 100% para una línea con una capacidad de 5.000 bps, y en torno al 71 por ciento para una línea de 7.000 bps de capacidad. En la parte (b) de la Figura 8.14 se muestra el retardo medio experimentado por una trama en función de la utilización y de la velocidad de datos. Se observa que, a medida que crece la utilización, lo hacen también los requisitos de almacenamiento temporal y el retardo. Resulta claramente no deseable una utilización por encima del 80 por ciento.

Obsérvese que el tamaño promedio para la memoria temporal sólo depende de ρ, y no directamente de M. Por ejemplo, considérense los dos casos siguientes:

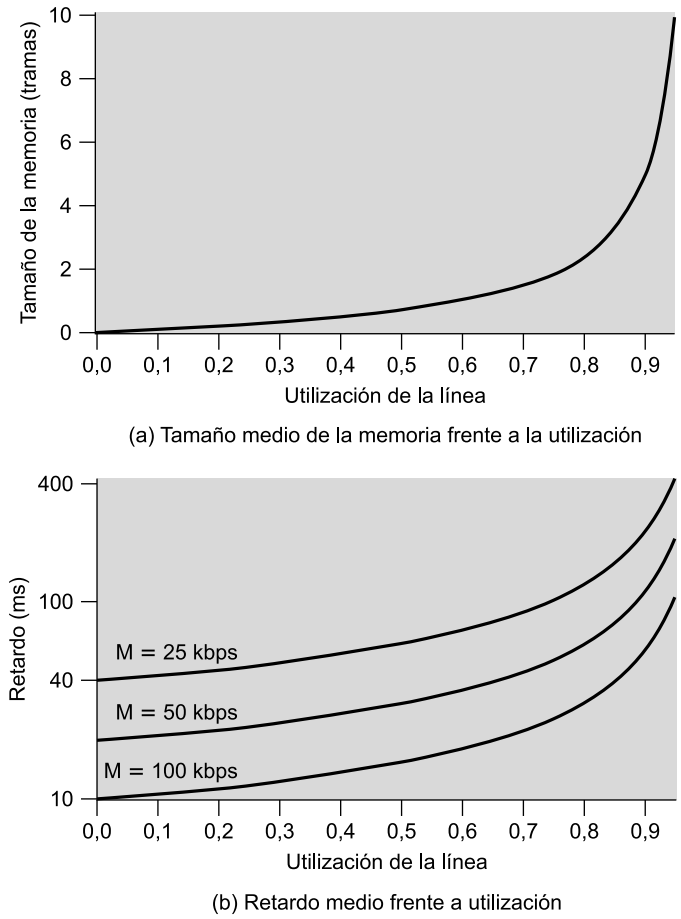


Figura 8.14. Tamaño de la memoria temporal y retardo para un multiplexor estadístico.

Caso I	Caso II
$I = 10$ $R = 100$ bps $\alpha = 0{,}4$ $M = 500$ bps	$I = 100$ $R = 100$ bps $\alpha = 0{,}4$ $M = 5.000$ bps

En ambas situaciones, el valor de ρ es 0,8 y el tamaño medio de la memoria temporal es $N = 2{,}4$. Así, para multiplexores que gestionan un número elevado de fuentes se requiere, proporcionalmente, una menor cantidad de memoria por fuente. En la Figura 8.14b se muestra también que el retardo promedio, para una utilización constante, será menor a medida que aumente la capacidad del enlace.

Hasta ahora se ha considerado la longitud promedia de cola y, en consecuencia, el tamaño medio de la memoria temporal necesaria. Es claro que existirá un límite superior para el tamaño de memoria temporal disponible. La varianza del tamaño de la cola aumenta con la utilización. Así, a mayor nivel de utilización, mayor será la memoria necesaria para gestionar el exceso. Aun así,

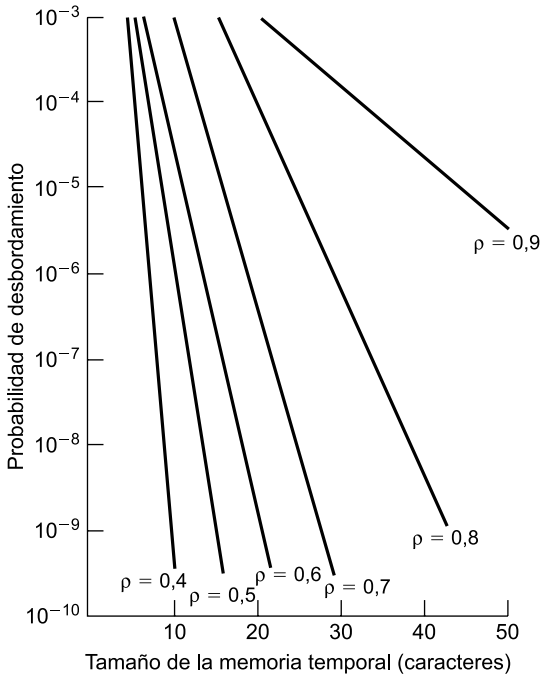


Figura 8.15. Probabilidad de desbordamiento de la memoria temporal en función de su tamaño.

existe siempre una probabilidad finita de que la memoria temporal se desborde. En la Figura 8.15 se muestra la fuerte dependencia de la probabilidad de desbordamiento de la memoria temporal con la utilización. Esta figura, junto con la Figura 8.14, sugiere que no es deseable una utilización por encima de 0,8.

CABLE-MÓDEM

Un proveedor de TV por cable dedica dos canales para dar soporte a la transferencia de datos desde y hacia un sistema de cable-módem, uno para la transmisión en cada dirección. Cada canal se comparte entre un número dado de abonados, de modo que se precisa algún esquema para realizar la reserva de capacidad en cada canal de transmisión. Como se muestra en la Figura 8.16, para ello se usa generalmente una variante del sistema TDM estadístico. En la dirección descendente (*downstream*), desde el **punto raíz** del sistema de cable hacia el abonado, un planificador envía datos en forma de pequeños paquetes. Dado que el canal es compartido por varios abonados, si más de uno de ellos se encuentra activo, cada abonado sólo conseguirá una fracción de la capacidad descendente. Un abonado de cable-módem individual puede conseguir velocidades de acceso comprendidas entre 500 kbps y 1,5 Mbps o más, dependiendo de la arquitectura de red y de la carga de tráfico. La dirección descendente se utiliza también para conceder ranuras temporales a los abonados. Cuando un abonado tiene datos que transmitir, en primer lugar debe solicitar ranuras temporales sobre el canal ascendente (*upstream*) compartido. Con este fin, a cada abonado se le conceden ranuras temporales dedicadas. El planificador raíz responde a un paquete de solicitud devolviendo una asignación de ranuras temporales futuras a usar por el abonado en cuestión. De esta forma, varios abonados pueden compartir el mismo canal ascendente sin entrar en conflicto.

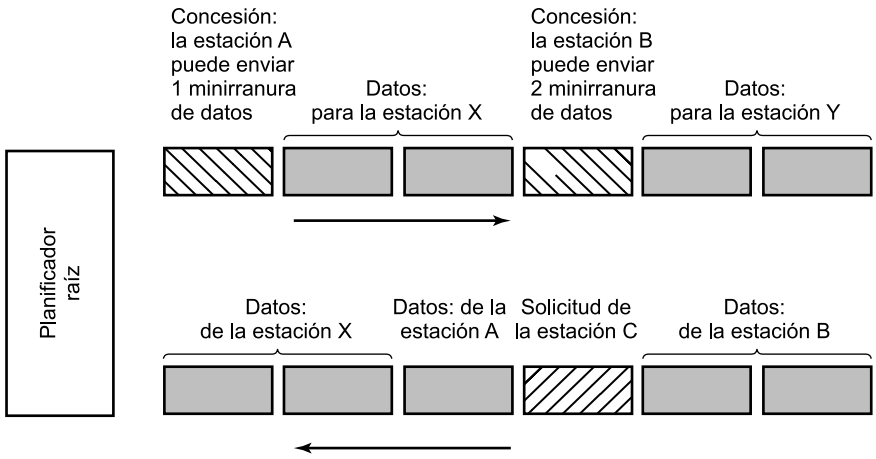


Figura 8.16. Esquema del sistema de cable-módem [DUTT99].

8.4. LÍNEA DE ABONADO DIGITAL ASIMÉTRICA

La parte que supone un mayor desafío en la implementación y desarrollo de una red digital pública de área amplia de alta velocidad es el enlace entre el abonado y la red: la línea de abonado digital. Dada la existencia de miles de millones de abonados potenciales en todo el mundo, la sola idea de llevar a cabo la instalación de nuevo cable para cada uno de los usuarios asusta. En lugar de ello, los diseñadores de redes han estudiado distintas formas de aprovechar el cable de par trenzado ya instalado y que enlaza con redes telefónicas prácticamente a todos los consumidores particulares y de empresa. Estos enlaces fueron instalados para transportar señales de voz en un ancho de banda de cero a 4 kHz. Sin embargo, los cables son capaces de transmitir señales con un espectro mucho más amplio (1 MHz o más).

ADSL es la más conocida de una nueva familia de tecnologías módem diseñada para permitir la transmisión de datos digitales a alta velocidad a través de cable telefónico convencional. ADSL está siendo ofrecida por varios proveedores y se encuentra definida en una normalización ANSI. En esta sección se verá en primer lugar el diseño completo de ADSL, tras lo cual se presentarán los fundamentos de la tecnología subyacente conocida como DMT.

DISEÑO ADSL

El término *asimétrico* se refiere al hecho de que ADSL proporciona más capacidad de transmisión en el enlace descendente (desde la oficina central del proveedor hacia el usuario) que en el ascendente (desde el usuario hacia el proveedor). ADSL se orientó originalmente hacia las necesidades de recursos previstas en aplicaciones de vídeo bajo demanda y servicios relacionados. A pesar de que este tipo de aplicaciones no se ha materializado, la demanda de acceso de alta velocidad a Internet ha crecido desde la aparición de la tecnología ADSL. En general, el usuario precisa mayor capacidad en el enlace descendente que para la transmisión ascendente. La mayor parte de las transmisiones realizadas por un usuario son del tipo de pulsaciones de teclado o transmisión de mensajes cortos de correo electrónico, mientras que el tráfico de entrada, especialmente el tráfico web, puede conllevar grandes cantidades de datos que incluyen imágenes e incluso vídeo. Es por ello que la tecnología ADSL resulta muy apropiada para las necesidades de transmisión en Internet.

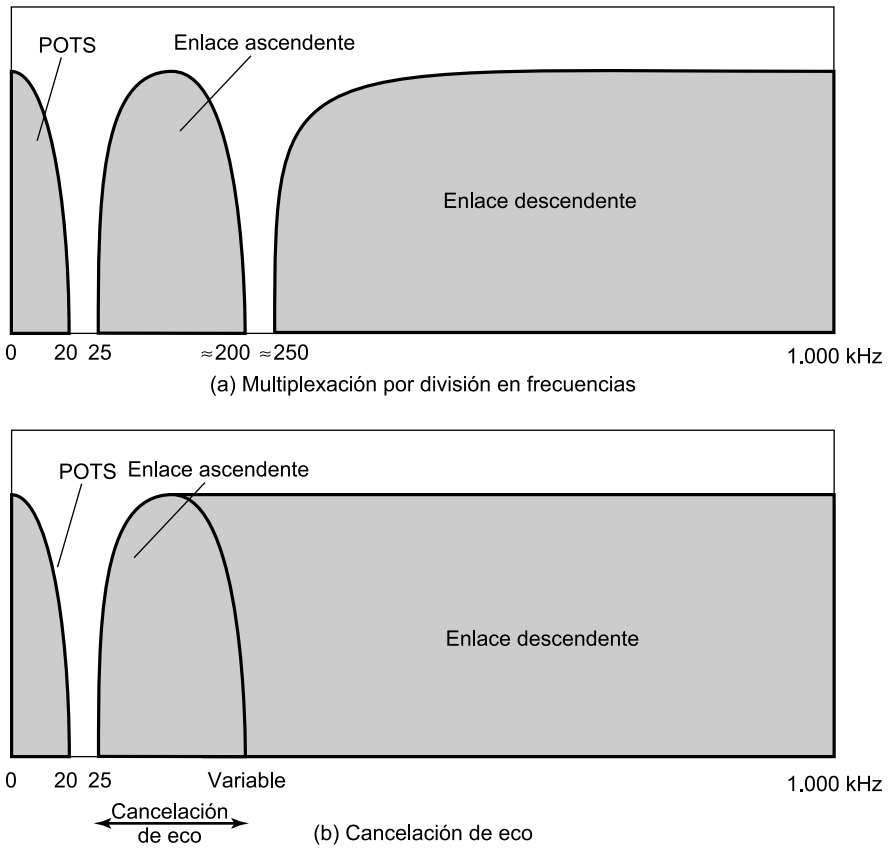


Figura 8.17. Configuración de canales ADSL.

ADSL hace uso de multiplexación por división en frecuencias (FDM) de una forma novedosa para aprovechar la capacidad de 1 MHz de que dispone el cable de par trenzado. Existen tres elementos en el esquema ADSL (*véase* Figura 8.17):

- Reserva de los 25 kHz inferiores para voz, conocido como POST (*Plain Old Telephone Service*). La voz se transmite sólo en la banda 0-4 kHz, sirviendo el ancho de banda adicional para evitar la producción de diafonía entre los canales de voz y de datos.
- Utilización de cancelación de eco[4] o FDM, para dar cabida a dos bandas, una ascendente pequeña y una descendente grande.
- Uso de FDM en las bandas ascendente y descendente. En este caso, una secuencia de bits dada se divide en varias secuencias paralelas y cada una de ellas se transmite en una banda de frecuencias distinta.

Cuando se usa cancelación de eco, la banda de frecuencia correspondiente al canal ascendente se solapa con la porción inferior del canal descendente. Este hecho presenta dos ventajas en

[4] La cancelación de eco es una técnica de procesamiento de señal que permite la transmisión de señales digitales en ambos sentidos de forma simultánea a través de una única línea de transmisión. En esencia, un transmisor debe eliminar de la señal que recibe el eco debido a su propia transmisión con objeto de recuperar la señal enviada por el otro extremo.

comparación con el empleo de bandas de frecuencia distintas para los enlaces ascendente y descendente:

- La atenuación aumenta con la frecuencia. Con la utilización de cancelación de eco, una mayor parte del ancho de banda del enlace descendente se encuentra en la zona «adecuada» del espectro.
- El diseño del procedimiento de cancelación de eco es más flexible para modificar la capacidad de la transmisión ascendente. Aunque este canal se puede extender hacia frecuencias superiores sin llegar a caer dentro del ancho de banda del canal descendente, lo que se hace es aumentar el área de solapamiento.

La desventaja del uso de la cancelación de eco es la necesidad de la existencia de lógica de cancelación de eco en ambos extremos de la línea.

El esquema ADSL permite distancias de hasta 5,5 km en función del diámetro del cable y de la calidad de éste. Esto resulta suficiente para dar servicio en torno al 95 por ciento de todos los bucles de abonado de Estados Unidos y del mismo orden en otros países.

MULTITONO DISCRETO

La técnica de multitono discreto (DMT, *Discrete MultiTone*) consiste en hacer uso de varias señales portadoras a diferentes frecuencias, de modo que se envían algunos de los bits en cada canal. El ancho de banda disponible (ascendente o descendente) se divide en varios subcanales de 4 kHz. En el proceso de inicialización, el módem DMT envía señales de test sobre los subcanales con el fin de determinar la relación señal-ruido en cada uno de ellos. Realizado el test, el módem asigna más bits de datos a los canales con mejor calidad de transmisión de señal y un número de bits menor para aquellos canales de calidad inferior. En la Figura 8.18 se ilustra este proceso. Cada subcanal puede transportar datos a una velocidad comprendida entre 0 y 60 kbps. La figura muestra una situación típica en la que existe un aumento de la atenuación y, por tanto, un decremento en la relación señal-ruido a altas frecuencias. En consecuencia, los subcanales de frecuencia superior transportan menos datos.

En la Figura 8.19 se ofrece un diagrama general de la transmisión DMT. Tras el proceso de inicialización, la secuencia de bits a transmitir se divide en varias subsecuencias, una para cada subcanal que transportará datos. La suma de las velocidades de las subsecuencias es igual a la velocidad total. A continuación, cada subsecuencia se convierte en una señal analógica mediante la técnica de modulación en amplitud en cuadratura (QAM), descrita en el Capítulo 5. Este esquema funciona adecuadamente gracias a la capacidad de QAM para asignar a cada uno de los elementos de señal transmitidos un número diferente de bits. Cada señal QAM ocupa una banda de frecuencia diferente, de modo que estas señales se pueden combinar sin más que sumarlas para dar lugar a la señal compuesta a transmitir.

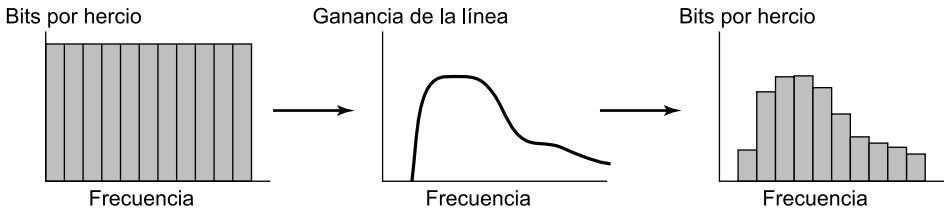


Figura 8.18. Reserva de bits por canal en DMT.

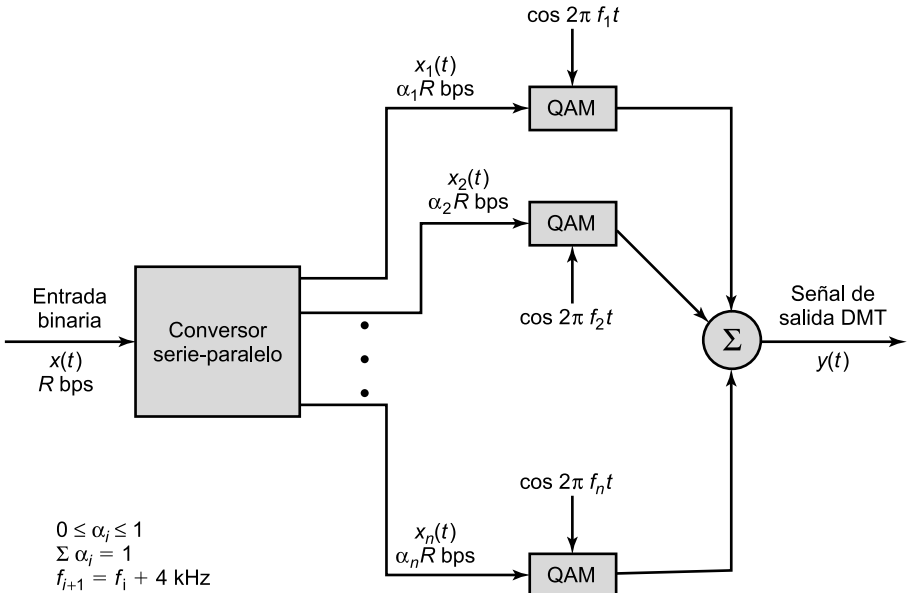


Figura 8.19. Transmisor DMT.

Los diseños ADSL/DMT actuales utilizan 256 subcanales descendentes. En teoría, con cada subcanal de 4 kHz transportando 60 kbps, sería posible transmitir a una velocidad de 15,36 Mbps. En cambio, en la práctica, el deterioro de la transmisión impide la consecución de esta velocidad. Las implementaciones actuales operan en el rango 1,5-9 Mbps dependiendo de la distancia de la línea y de la calidad de ésta.

8.5. xDSL

ADSL es uno de los numerosos esquemas de reciente aparición para proporcionar una transmisión digital a alta velocidad sobre el bucle de abonado. En la Tabla 8.8 se resumen y comparan algunos de los más importantes de estos nuevos esquemas, los cuales se denominan de forma genérica xDSL.

LÍNEA DE ABONADO DIGITAL DE ALTA VELOCIDAD (HDSL)

HDSL se desarrolló a finales de la década de 1980 por BellCore con objeto de ofrecer una forma más efectiva, desde el punto de vista del coste, para el envío de datos a la velocidad proporcionada por T1 (1,544 Mbps). La línea estándar T1 usa codificación AMI, que ocupa un ancho de banda de alrededor de 1,5 MHz. Debido a la aparición de estas altas frecuencias, las características de atenuación limitan el uso de T1 para distancias de en torno a 1 km entre repetidores. Por tanto, para muchos de los bucles de abonado se precisan uno o más repetidores, lo cual encarece la instalación y su mantenimiento.

En HDSL se hace uso del esquema de codificación 2B1Q para poder alcanzar una velocidad de datos de hasta 2 Mbps a través de dos líneas de par trenzado dentro de un ancho de banda que se extiende sólo hasta, aproximadamente, 196 kHz. Para conseguir esto se trabaja con distancias en torno a 3,7 km.

Tabla 8.8. Comparación de las técnicas xDSL.

	ADSL	HDSL	SDSL	VDSL
Bits/segundo	de 1,5 a 9 Mbps en descendente de 16 a 640 kbps en ascendente	1,544 o 2,048 Mbps	1,544 o 2,048 Mbps	de 13 a 52 Mbps en descendente de 1,5 a 2,3 Mbps en ascendente
Modo	Asimétrico	Simétrico	Simétrico	Asimétrico
Pares de cobre	1	2	1	1
Distancia (UTP de calibre 24)	de 3,7 a 5,5 km	3,7 km	3,0 km	1,4 km
Señalización	Analógica	Digital	Digital	Analógica
Código de línea	CAP/DMT	2B1Q	2B1Q	DMT
Frecuencia	de 1 a 5 MHz	196 kHz	196 kHz	10 MHz
Bits/ciclo	Variable	4	4	Variable

UTP = par trenzado sin apantallar.

LÍNEA DE ABONADO DIGITAL DE UNA SOLA LÍNEA (SDSL)

Aunque HDSL resulta atractiva para reemplazar las líneas T1 existentes, ello no es posible para abonados particulares ya que en HDSL se precisan dos pares trenzados y estos abonados disponen generalmente de un solo par. Así, SDSL se desarrolló para proporcionar a través de una única línea de par trenzado el mismo tipo de servicio que HDSL proporciona con dos. Como en el caso de HDSL, en SDSL se usa la técnica de codificación 2B1Q. Se emplea cancelación de eco para conseguir transmisión *full-duplex* a través de un único par.

LÍNEA DE ABONADO DIGITAL DE MUY ALTA VELOCIDAD (VDSL)

Uno de los esquemas xDSL más recientes es VDSL. Muchos de los detalles de esta especificación de señalización se encuentran aún por definir en el momento de la escritura de este texto. El objetivo de VDSL es proveer un esquema similar a ADSL a una velocidad muy superior, a costa de disminuir la distancia permitida. La técnica de señalización para VDSL será probablemente DMT/QAM.

VDSL no utiliza cancelación de eco, pero proporciona bandas separadas para los diferentes servicios, siendo la asignación provisional para cada uno de ellos la siguiente:

- POTS: 0-4 kHz
- RDSI: 4-80 kHz
- Enlace ascendente: 300-700 kHz
- Enlace descendente: $\geqslant$ 1 MHz

8.6. LECTURAS Y SITIOS WEB RECOMENDADOS

En [BELL90] y [FREE98] puede encontrarse un estudio sobre los sistemas de transmisión TDM y FDM. Por su parte, en [STAL99] se tratan en mayor profundidad las interfaces RDSI y SONET.

El texto [MAXW96] proporciona un excelente estudio sobre ADSL. Se recomiendan [HAWL97] y [HUMP97] por el tratamiento de las técnicas xDSL que en ellos se hace.

BELL90 Bellcore (Bell Communications Research). *Telecommunications Transmission Engineering*. Tres volúmenes, 1990.

FREE98 Freeman, R. *Telecommunications Transmission Handbook*. New York: Wiley, 1998.

HAWL97 Hawley, G. «Ssystems Considerations for the Use of xDSL Technology for Data Access.» *IEEE Communications Magazine*, marzo 1997.

HUMP97 Humphrey, M., y Freeman, J. «How xDSL Supports Broadband Services to the Home.» *IEEE Network*, enero/marzo 1997.

MAXW96 Maxwell, K. «Asymmetric Digital Subscriber Line: Interim Technology for the Next Forty Years.» *IEEE Communications Magazine*, octubre 1996.

STAL99 Stallings, W. *ISDN and Broadband ISDN, with Frame Relay and ATM*. Upper Saddle River, NJ: Prentice Hall, 1999.

SITIOS WEB RECOMENDADOS

- **Foro ADSL:** incluye una lista de FAQ (*Frequently Asked Questions*) e información técnica sobre ADSL y otras tecnologías xDSL.
- **Foro de integración de redes y servicios:** presenta productos, tecnologías y estándares actuales relacionados con SONET.
- **Página principal de SONET:** enlaces de interés, artículos especializados, informes oficiales y preguntas planteadas habitualmente (FAQ).

8.7. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

ADSL
cable-módem
canal
canal ascendente
canal descendente
cancelación de eco
demultiplexor
inserción de bits
multiplexación
multiplexación por división en el tiempo (TDM)
multiplexación por división en frecuencias (FDM)
multiplexor
multitono discreto
SDH
sistema de portadora digital
SONET
subportadora
TDM estadística
TDM síncrona
trama

CUESTIONES DE REPASO

8.1. ¿Por qué es efectiva la multiplexación desde el punto de vista del coste?

8.2. ¿Cómo se evita la aparición de interferencias haciendo uso de la técnica de multiplexación por división en frecuencias?

8.3. ¿Qué es la cancelación de eco?

8.4. Defina *canal ascendente* y *canal descendente* en el contexto de las líneas de abonado.

8.5. Explique cómo funciona la técnica de multiplexación por división en el tiempo síncrona (TDM).

8.6. ¿Por qué es más eficiente un multiplexor por división en el tiempo estadístico que uno síncrono?

8.7. Basándose en la Tabla 8.3, indique la principal diferencia entre los sistemas TDM de Norteamérica e Internacional.

8.8. En base a la Figura 8.14, indique la relación entre el tamaño de las memorias temporales y la utilización de línea.

EJERCICIOS

8.1. La información correspondiente a cuatro señales analógicas se multiplexa y transmite a través de un canal telefónico con una banda de paso de 400 a 3.100 Hz. Cada una de las señales analógicas en banda base está limitada en banda hasta 500 Hz. Diseñe un sistema de comunicaciones (a nivel de diagrama de bloques) que permita la transmisión de estas cuatro fuentes a través del canal telefónico haciendo uso de:

a) Multiplexación por división en frecuencias con subportadoras SSB (banda lateral única, *Single SideBand*).

b) Multiplexación por división en el tiempo usando PCM, considerando 4 bits por muestra.

Dibuje los diagramas de bloques del sistema completo en ambos casos, incluyendo las partes de transmisión, canal y recepción. Incluya los anchos de banda de las señales en los distintos puntos del sistema.

8.2. Parafraseando a Lincoln, «...todo el canal durante algún tiempo, parte del canal durante todo el tiempo...». Relacione esta frase con la Figura 8.2.

8.3. Considere un sistema de transmisión que hace uso de multiplexación por división en frecuencias. ¿Qué factores de coste se verán afectados al añadir uno o más pares de estaciones al sistema?

8.4. En TDM síncrona es posible entremezclar los bits, considerando para ello un bit de cada canal en cada ciclo. Si los canales usan un código de auto-reloj (es decir, la señal de reloj está contenida en el propio código) para facilitar la sincronización, ¿podría esta mezcla de bits introducir problemas debido a que no existe una secuencia continua de bits procedente de cada una de las fuentes?

8.5. ¿Por qué se pueden eliminar los bits de comienzo y de parada cuando se usa mezcla de caracteres en TDM síncrona?

8.6. Explique, desde el punto de vista del control del enlace de datos y de la capa física, cómo se realizan el control de flujo y el control de errores en la multiplexación por división en el tiempo síncrona.

8.7. Uno de los 193 bits en el formato de transmisión DS-1 se usa para sincronización de trama. Explique su funcionamiento.

8.8. ¿Cuál es la velocidad de la señalización de control para cada canal de voz en el formato DS-1?

8.9. Se multiplexan y transmiten 24 señales de voz a través de un par trenzado. ¿Cuál es el ancho de banda necesario en FDM? Suponiendo una eficiencia del ancho de banda (relación entre la velocidad de datos y el ancho de banda de la transmisión, ya explicada en el Capítulo 5) de 1 bps/Hz, ¿cuál es el ancho de banda necesario para TDM haciendo uso de PCM?

8.10. Dibuje un diagrama de bloques similar al de la Figura 8.8 para un sistema TDM PCM que dé cabida a cuatro entradas digitales síncronas a 300 bps y una entrada analógica con un ancho de banda de 500 Hz. Suponga que las muestras analógicas se codifican en palabras PCM de 4 bits.

8.11. Se utiliza un multiplexor por división en el tiempo con mezcla de caracteres para combinar las secuencias de datos procedentes de varios terminales asíncronos a 110 bps para transmisión de datos sobre una línea digital de 2.400 bps. Cada terminal envía caracteres asíncronos de 7 bits de datos, 1 bit de paridad, 1 bit de comienzo y 2 bits de parada. Suponga que se envía un carácter de sincronización cada 19 caracteres de datos y que, al menos, el 3 por ciento de la capacidad de la línea se reserva para la inserción de bits con objeto de adaptar las variaciones de velocidad de los distintos terminales.

a) Determine el número de bits por carácter.

b) Calcule el número de terminales que puede servir el multiplexor.

c) Obtenga un posible patrón de delimitación para el multiplexor.

8.12. Encuentre el número de dispositivos, especificados a continuación, que puede atender una línea TDM de tipo T1 si el 1 por ciento de la capacidad de la línea se reserva con fines de sincronización.

a) Terminales teletipo a 110 bps.

b) Terminales de computador a 300 bps.

c) Terminales de computador a 1.200 bps.

d) Puertos de salida de computador a 9.600 bps.

e) Líneas de voz PCM a 64 kbps.

¿Cómo variaría este número si cada una de las fuentes estuviese operativa en promedio el 10 por ciento del tiempo y se utilizase un multiplexor estadístico?

8.13. Se multiplexan 10 líneas a 9.600 bps haciendo uso de TDM. Ignorando los bits suplementarios en la trama TDM, ¿cuál es la capacidad total requerida para TDM síncrona? Suponiendo que deseamos limitar la utilización media de línea a 0,8, y suponiendo que cada línea está ocupada el 50 por ciento del tiempo, ¿cuál es la capacidad necesaria en TDM estadística?

8.14. Se usa un esquema TDM síncrono para la combinación y transmisión de cuatro señales a 4,8 kbps y una a 9,6 kbps sobre una línea alquilada. Con fines de delimitación, se incluye un bloque de 7 bits (patrón 1011101) cada 48 bits de datos. El algoritmo de redelimitación (en el demultiplexor receptor) es como sigue:

1. Se selecciona una posición de bit arbitraria.

2. Se considera el bloque de 7 bits contiguo comenzando en dicha posición.

3. Se comprueba dicho bloque de 7 bits para cada una de las 12 tramas consecutivas.

4. Si se encuentra el patrón de delimitación en 10 de los 12 bloques el sistema está «en trama»; en caso contrario, se avanza una posición de bit y se vuelve al paso 2.

a) Dibuje la secuencia de bits multiplexada (obsérvese que la entrada a 9,6 kbps se puede tratar como dos entradas a 4,8 kbps).

b) ¿Cuál es el porcentaje de información suplementaria en la secuencia de bits multiplexada?

c) ¿Cuál es la velocidad de salida multiplexada?

d) ¿Cuál es el tiempo de redelimitación mínimo? ¿Y el máximo? ¿Y su valor promedio?

8.15. Una compañía tiene dos sedes: la oficina central y una fábrica en torno a unos 25 km de la primera. La fábrica tiene cuatro terminales a 300 bps que se comunican con los servicios computacionales del computador central sobre líneas alquiladas de calidad telefónica. La compañía está planteándose la instalación de equipos TDM, de modo que sólo se precise una línea. ¿Qué factores de coste deben considerarse en la toma de la decisión?

8.16. En TDM síncrona, las líneas de entrada/salida servidas por los dos multiplexores pueden ser síncronas o asíncronas, aunque el canal entre los multiplexores debe ser síncrono. ¿Existe alguna inconsistencia en esta afirmación? Razone la respuesta.

8.17. Suponga que está diseñando un sistema TDM, digamos DS-489, para dar servicio a 30 canales de voz usando muestras de 6 bits y una estructura similar a DS-1. Determine la velocidad requerida.

8.18. Se definen los siguientes parámetros para un multiplexor por división en el tiempo estadístico:

F = longitud de la trama, en bits
OH = información suplementaria en una trama, en bits
L = carga útil de datos en la trama, en bps
C = capacidad del enlace, en bps

a) Exprese F en función de los otros parámetros. Explique por qué se puede ver F más como una variable que como una constante.

b) Represente gráficamente F frente a L para $C = 9{,}6$ kbps y para valores de $OH = 40$, 80 y 120. Comente los resultados y compárelos con los de la Figura 8.14.

c) Dibuje F en función de L para $OH = 40$ y para valores de $C = 9{,}6$ kbps y 8,2 kbps. Comente los resultados y compárelos con los de la Figura 8.14.

8.19. En TDM estadística puede existir un campo de longitud ¿Qué alternativa se puede considerar a la inclusión de este campo? ¿Qué problema podría ocasionar esta solución y cómo se puede resolver?

CAPÍTULO 9

Espectro expandido

9.1. El concepto de espectro expandido

9.2. Espectro expandido por salto de frecuencias
Esquema básico
FHSS usando MFSK
Análisis de prestaciones de FHSS

9.3. Espectro expandido de secuencia directa
DSSS usando BPSK
Análisis de prestaciones de DSSS

9.4. Acceso múltiple por división de código
Principios básicos
CDMA para espectro expandido de secuencia directa

9.5. Lecturas recomendadas

9.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- La técnica de espectro expandido constituye una forma de codificación cada vez más importante en comunicaciones inalámbricas. El empleo de este esquema dificulta las interferencias y la intercepción, al tiempo que mejora la recepción.
- La idea básica del esquema de espectro expandido es la modulación de la señal, de modo que se incremente de manera significativa el ancho de banda (expansión del espectro) de la señal a transmitir.
- La técnica de **espectro expandido por salto de frecuencias** es una variante en la que la señal se transmite sobre una serie aparentemente aleatoria de radiofrecuencias, saltando de frecuencia en frecuencia en intervalos temporales fijos.
- La técnica de **espectro expandido de secuencia directa** es una variante en la que cada bit de la señal original se representa mediante varios bits en la señal transmitida, a través del empleo de un código de expansión.
- El **acceso múltiple por división de código** aprovecha la naturaleza de la transmisión de espectro expandido para posibilitar a varios usuarios utilizar de forma independiente el mismo ancho de banda con muy pocas interferencias.

El esquema de espectro expandido constituye una forma de codificación cada vez más importante en comunicaciones inalámbricas. Esta técnica no se puede encuadrar dentro de las categorías definidas en el Capítulo 5, puesto que puede utilizarse para transmitir tanto datos analógicos como digitales, haciendo uso de una señal analógica.

La técnica de espectro expandido fue originalmente desarrollada con objetivos militares y de inteligencia. La idea esencial subyacente en este tipo de esquema es la expansión de la señal de información en un ancho de banda superior con objeto de dificultar las interferencias y la intercepción. La primera variante de espectro expandido desarrollada fue la denominada por salto de frecuencias[1]. Una forma más reciente de espectro expandido es la de secuencia directa. Ambas variantes se utilizan en numerosos estándares y productos en comunicaciones inalámbricas.

Tras una breve discusión, se examinarán ambos tipos de esquemas de espectro expandido. Seguidamente se estudiará una técnica de acceso múltiple basada en el esquema de espectro expandido.

9.1. EL CONCEPTO DE ESPECTRO EXPANDIDO

La Figura 9.1 destaca las características principales de un sistema de espectro expandido. La entrada va a un codificador de canal que produce una señal analógica con un ancho de banda relativamente estrecho centrado en una frecuencia dada. Esta señal se modula posteriormente haciendo uso de una secuencia de dígitos conocida como código o secuencia de expansión. Generalmente, aunque no siempre, el código expansor se genera mediante un generador de pseudoruido o números pseudoaleatorios. El efecto de esta modulación es un incremento significativo en el ancho de banda

[1] Por increíble que pueda parecer, la técnica de espectro expandido (por salto de frecuencias) fue inventada por la estrella de Hollywood Hedy Lamarr en 1940, a los 26 años de edad. Ella, junto con un socio, consiguieron una patente en 1942 («U.S. patent 2.292.387», el 11 de agosto de 1942). Lamarr consideró que ésa iba a ser su contribución a la causa de la guerra, no obteniendo nunca beneficios por su invención.

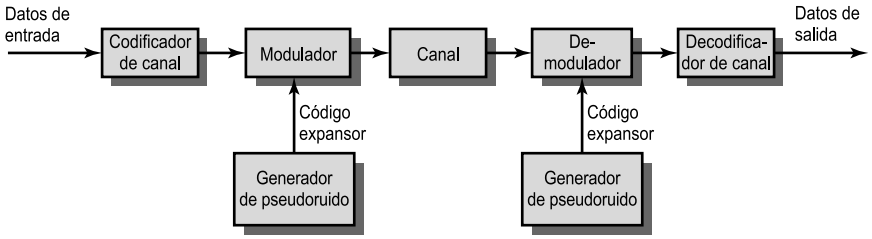


Figura 9.1. Modelo general de un sistema de comunicación digital de espectro expandido.

(expansión del espectro) de la señal a transmitir. El extremo receptor usa la misma secuencia pseudoaleatoria para demodular la señal de espectro expandido. Finalmente, la señal pasa a un decodificador de señal a fin de recuperar los datos.

A través de este aparente desaprovechamiento de espectro se consigue:

- Más inmunidad ante diversos tipos de ruido y distorsión multitrayectoria. Las primeras aplicaciones del esquema de espectro expandido eran militares, donde se usaba por su inmunidad a interferencias.
- También puede utilizarse para ocultar y cifrar señales. Sólo un usuario que conozca el código expansor podrá recuperar la información codificada.
- Varios usuarios independientes pueden utilizar el mismo ancho de banda con muy pocas interferencias entre sí. Esta propiedad es usada en aplicaciones de telefonía celular a través del empleo de una técnica conocida como multiplexación por división de código (CDM, *Code Division Multiplexing*) o acceso múltiple por división de código (CDMA, *Code Division Multiple Access*).

Se impone un comentario acerca de los números pseudoaleatorios. Estos números son generados por un algoritmo que utiliza un valor inicial llamado semilla. El algoritmo es determinista y, por tanto, genera secuencias de números que no son estadísticamente aleatorios; sin embargo, si el algoritmo es adecuado, dichas secuencias pueden superar diversos tests de aleatoriedad. Estos números se denominan a veces pseudoaleatorios[2] y su principal característica radica en el hecho de que, a menos que se conozca el algoritmo y la semilla, es prácticamente imposible predecir la secuencia correspondiente. Por tanto, sólo un receptor que comparta esta información con el emisor está capacitado para decodificar correctamente la señal.

9.2. ESPECTRO EXPANDIDO POR SALTO DE FRECUENCIAS

En el esquema de espectro expandido por salto de frecuencias (FHSS, *Frequency Hopping Spread Spectrum*), la señal se emite sobre una serie de radiofrecuencias aparentemente aleatoria, saltando de frecuencia en frecuencia en intervalos fijos de tiempo. El receptor captará el mensaje saltando de frecuencia en frecuencia síncronamente con el transmisor. Por su parte, los receptores no autorizados escucharán una señal ininteligible. Si se intentase interceptar la señal, sólo se conseguiría para unos pocos bits.

[2] *Véase* [STAL02] para un estudio más detallado acerca de números pseudoaleatorios.

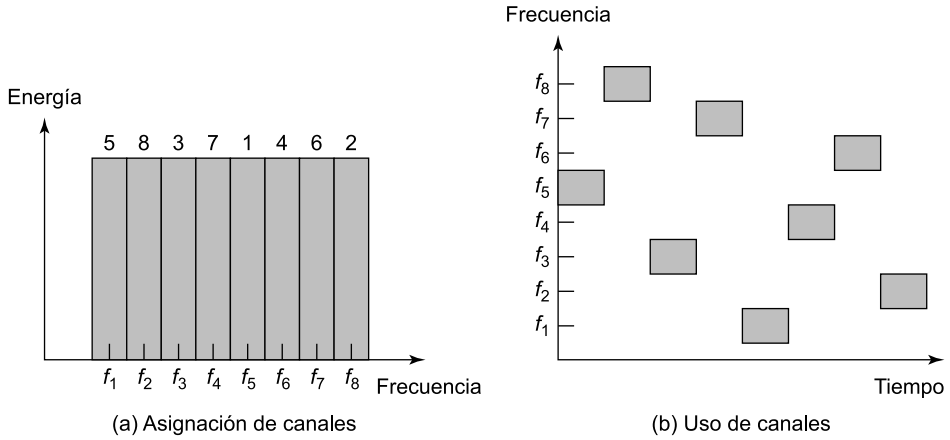


Figura 9.2. Ejemplo de salto de frecuencias.

ESQUEMA BÁSICO

El diagrama típico de un sistema basado en salto de frecuencias se muestra en la Figura 9.2. Se reservan varios canales para la señal FH, existiendo por lo general 2^k frecuencias portadoras que dan lugar a 2^k canales. El espaciado entre frecuencias portadoras y, por tanto, el ancho de banda de cada canal, se corresponde generalmente con el de la señal de entrada. El emisor opera en un canal durante un intervalo fijo (por ejemplo, el estándar IEEE 802.11 considera un intervalo de 300 ms). Durante este intervalo se transmiten varios bits (posiblemente correspondientes a una fracción de un bit, como veremos más adelante) haciendo uso de algún esquema de codificación. La secuencia de canales queda especificada por un código expansor, utilizando el emisor y el receptor el mismo a fin de sincronizar la secuencia de canales seguida.

En la Figura 9.3 se muestra un diagrama de bloques típico correspondiente a un sistema basado en salto de frecuencias. En la transmisión, los datos binarios constituyen la entrada de un modulador que usa algún tipo de esquema de codificación digital a analógico, como por ejemplo desplazamiento en frecuencias (FSK, *Frequency Shift Keying*) o desplazamiento en fase binario (BPSK, *Binary Phase Shift Keying*). La señal resultante estará centrada en torno a una frecuencia base. Se utiliza un generador de números pseudoaleatorios o pseudoruido (PN, *pseudonoise*) que servirá como puntero en una tabla de frecuencias; éste es el código expansor referido anteriormente. Cada k bits del generador PN especifican una de las 2^k frecuencias portadoras, seleccionándose una nueva frecuencia en cada intervalo sucesivo (cada k bits PN). Esta frecuencia es modulada por la señal generada en el modulador inicial, dando lugar a una nueva señal con la misma forma pero ahora centrada en torno a la frecuencia elegida. En el receptor, la señal de espectro expandido se demodula haciendo uso de la misma secuencia de frecuencias derivadas de PN y, posteriormente, se demodula la señal resultante para producir los datos de salida.

La Figura 9.3 indica que las dos señales se multiplican. Veamos un ejemplo de funcionamiento haciendo uso del esquema de modulación BFSK. Podemos definir la entrada FSK al sistema FHSS [compárese con la Ecuación (5.3)] como:

$$s_d(t) = A\cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f)t) \quad \text{para} \quad iT < t < (i+1)T$$

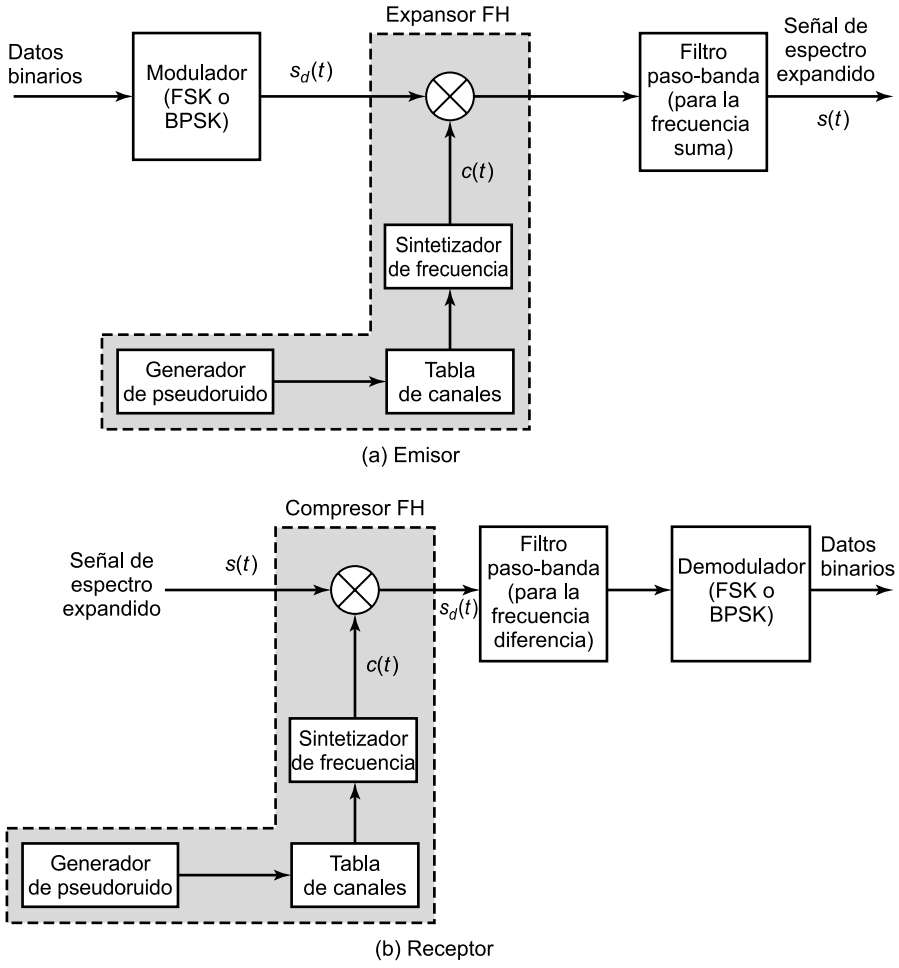


Figura 9.3. Sistema de espectro expandido por salto de frecuencias.

donde

A = amplitud de la señal.

f_0 = frecuencia base.

b_i = valor del i-ésimo bit de datos ($+1$ para el valor binario 1, -1 para el 0).

Δf = separación en frecuencia.

T = duración de bit; velocidad = $1/T$.

De este modo, durante el i-ésimo intervalo de bit, la frecuencia de la señal de datos es f_0 si el bit de datos es -1 y $f_0 + \Delta f$ si el bit de datos es $+1$.

El sintetizador de frecuencias genera un tono a frecuencia constante cuya frecuencia salta entre un conjunto de 2^k frecuencias posibles, estando determinado el patrón de salto por k bits de la secuencia PN. Por simplicidad, se supone que la duración de un salto es la misma que la de un bit y se ignoran diferencias de fase entre la señal de datos, $s_d(t)$, y la señal expandida, también llamada

señal de minibits («chips»), $c(t)$. Así, la señal producto durante el i-ésimo salto (durante el i-ésimo bit) es

$$p(t) = s_d(t)c(t) = A\cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f)t)\cos(2\pi f_i t)$$

donde f_i es la frecuencia de la señal generada por el sintetizador de frecuencias durante el i-ésimo salto. Haciendo uso de la identidad trigonométrica[3] $\cos(x)\cos(y) = (1/2)(\cos(x+y)+\cos(x-y))$, tendremos

$$p(t) = 0{,}5A[\cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f + f_i)t) + \cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f - f_i)t)]$$

Se utiliza un filtro paso-banda (*véase* la Figura 9.3) para eliminar la frecuencia diferencia y preservar la frecuencia suma, dando lugar a una señal FHSS:

$$s(t) = 0{,}5A\cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f + f_i)t)$$

De este modo, durante el intervalo del bit i-ésimo la frecuencia de la señal de datos será $f_0 + f_i$ si el bit de datos es -1 y $f_0 + f_i + \Delta f$ si el bit de datos es $+1$.

En el receptor se recibirá una señal de la forma $s(t)$ definida previamente, la cual se multiplicará por una réplica de la señal expandida para obtener una señal producto de la forma

$$p(t) = s(t)c(t) = 0{,}5A\cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f + f_i)t)\cos(2\pi f_i t)$$

Recurriendo de nuevo a la identidad trigonométrica, tendremos

$$p(t) = s(t)c(t) = 0{,}25A[\cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f + f_i + f_i)t) + \cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f)t)]$$

Se usa un filtro paso-banda (*véase* la Figura 9.3) para eliminar la frecuencia suma y preservar la frecuencia diferencia, dando lugar a una señal de la forma $s_d(t)$ definida en la Ecuación (9.1):

$$0{,}25A\cos(2\pi(f_0 + 0{,}5(b_i + 1)\Delta f)t)$$

FHSS USANDO MFSK

Una técnica de modulación usual empleada en conjunción con FHSS es la llamada FSK múltiple (MFSK). Recuérdese del Capítulo 5 que MFSK utiliza $M = 2^L$ frecuencias diferentes para codificar L bits de entrada de una vez. La señal transmitida es de la forma (Ecuación 5.4):

$$s_i(t) = A\cos 2\pi f_i t, \qquad 1 \leqslant i \leqslant M$$

donde

$f_i = f_c + (2i - 1 - M)f_d$

f_c = frecuencia portadora.

f_d = frecuencia diferencia.

M = número de elementos de señal distintos = 2^L.

L = número de bits por elemento de señal.

[3] *Véase* el documento WilliamStallings.com/StudentSupport.html como resumen de las identidades trigonométricas.

Para FHSS, la señal MFSK se traslada a una nueva frecuencia cada T_c segundos mediante la modulación de la señal MFSK con la señal portadora FHSS. El efecto es la traslación de la señal MFSK al canal FHSS apropiado. Para una velocidad R, la duración de un bit es $T = 1/R$ segundos y la duración de un elemento de señal $T_s = LT$ segundos. Si T_c es mayor o igual que T_s, la modulación expandida se denomina espectro expandido por salto de frecuencias lento; en caso contrario, se denominará espectro expandido por salto de frecuencias rápido[4]. En resumen,

Espectro expandido por salto de frecuencias lento	$T_c \geqslant T_s$
Espectro expandido por salto de frecuencias rápido	$T_c < T_s$

En la Figura 9.4 se muestra un ejemplo de FHSS lento, haciendo uso del esquema MFSK de la Figura 5.9. Se tiene $M = 4$, lo que significa que se usan cuatro frecuencias distintas para codificar 2 bits de entrada a la vez. Cada elemento de señal es un tono de frecuencia discreto y el ancho de banda total MFSK es $W_d = Mf_d$. Se hace uso de un esquema FHSS con $k = 2$, es decir, existen $4 = 2^k$ canales diferentes, cada uno de ancho W_d. El ancho de banda total del esquema FHSS es $W_s = 2^k W_d$. Cada 2 bits de la secuencia PN se utilizan para elegir uno de los cuatro canales, ocupándose el canal en cuestión durante un intervalo de dos elementos de señal, o cuatro bits ($T_c = 2T_s = 4T$).

En la Figura 9.5 se muestra un ejemplo de FHSS rápido haciendo uso del mismo esquema MFSK. Como antes, $M = 4$ y $k = 2$. Sin embargo, en este caso, cada elemento de señal se representa mediante dos tonos de frecuencia. De nuevo, $W_d = Mf_d$ y $W_s = 2^k W_d$. En este ejemplo, $T_c = 2T_s = 2T$. En general, FHSS rápido presenta unas mejores prestaciones que FHSS lento frente al ruido o las interferencias. Por ejemplo, si se usasen tres o más frecuencias («chips») para cada elemento de señal, el receptor podría decidir que el elemento de señal enviado es aquel para el que se obtiene una mayor cantidad de minibits correctos.

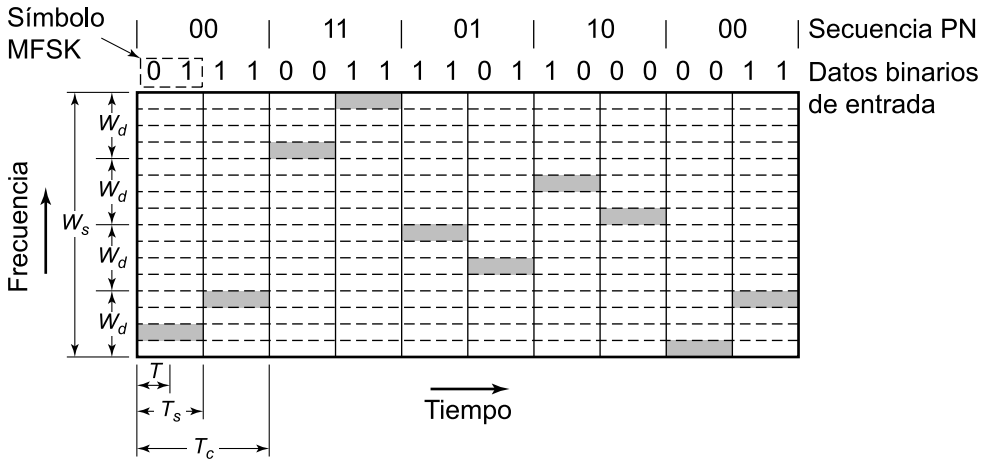


Figura 9.4. Espectro expandido por salto de frecuencias lento usando MFSK ($M = 4$, $k = 2$).

[4] Algunos autores utilizan una definición ligeramente diferente (por ejemplo, [PICK82]): varios saltos por bit en el caso de salto de frecuencias rápido, varios bits por salto en el salto de frecuencias lento y un salto por bit en otro caso. La definición más usual, que nosotros emplearemos, relaciona saltos con elementos de la señal en lugar de con bits.

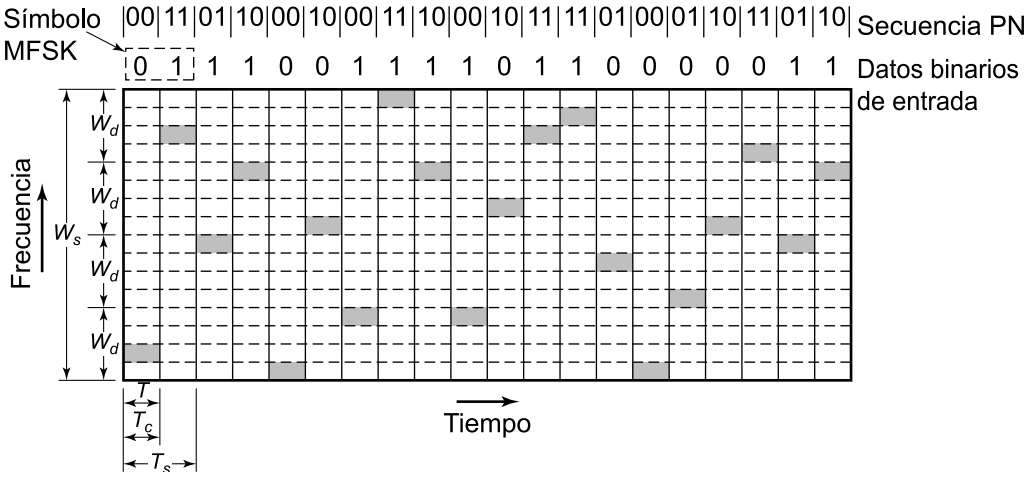


Figura 9.5. Espectro expandido por salto de frecuencias rápido usando MFSK ($M = 4$, $k = 2$).

ANÁLISIS DE PRESTACIONES DE FHSS

Por lo general se usa un gran número de frecuencias en FHSS, de modo que W_s es muy superior a W_d. Una ventaja de este hecho es que el uso de un valor de k elevado da lugar a sistemas altamente inmunes a interferencias. Por ejemplo, supongamos que tenemos un emisor MFSK con ancho de banda W_d e interferencias de ruido del mismo ancho de banda y potencia fija S_j sobre la frecuencia portadora de señal. Entonces, se tendrá una relación de energía de señal por bit frente a densidad de potencia del ruido por hercio de

$$\frac{E_b}{N_j} = \frac{E_b W_d}{S_j}$$

Si se usa el esquema de salto de frecuencias, la interferencia debe afectar a las 2^k frecuencias. Si la potencia es fija, esto reduce la potencia de la interferencia en cualquier banda de frecuencias a $S_j/2^k$. La ganancia en la relación señal-ruido, o ganancia de procesamiento, es

$$G_P = 2^k = \frac{W_s}{W_d}$$

9.3. ESPECTRO EXPANDIDO DE SECUENCIA DIRECTA

En el esquema de espectro expandido de secuencia directa (DSSS, *Direct Sequence Spread Spectrum*), cada bit de la señal original se representa mediante varios bits en la señal transmitida, haciendo uso de un código de expansión. Este código expande la señal sobre una banda de frecuencias más ancha de forma directamente proporcional al número de bits considerados. Es decir, un código de expansión de 10 bits expande la señal a una banda de frecuencias de anchura 10 veces mayor que un código de expansión de 1 bit.

Una técnica de espectro expandido de secuencia directa consiste en combinar la secuencia digital de entrada con el código expansor mediante la función or-exclusiva (XOR), la cual cumple las siguientes reglas:

$$0 \oplus 0 = 0 \qquad 0 \oplus 1 = 1 \qquad 1 \oplus 0 = 1 \qquad 1 \oplus 1 = 0$$

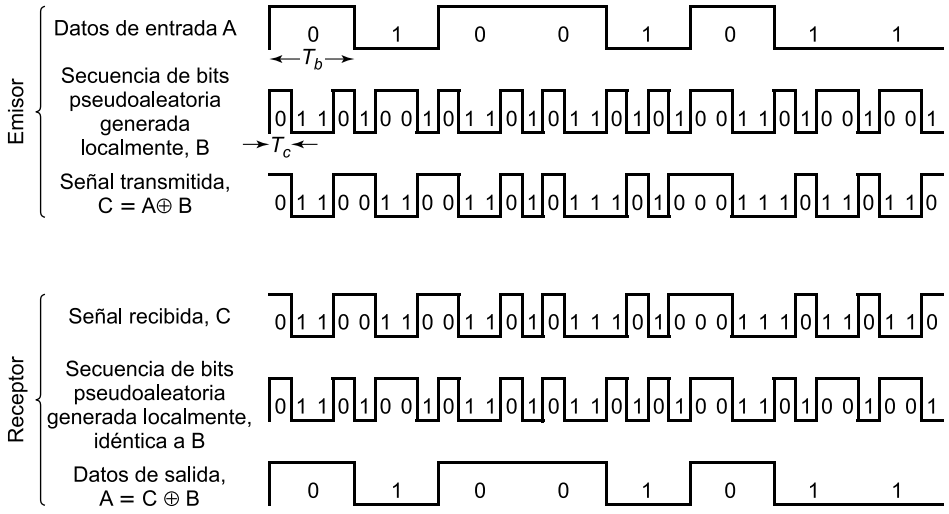

Emisor
Datos de entrada A
0 1 0 0 1 0 1 1
T_b
Secuencia de bits pseudoaleatoria generada localmente, B
0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 1 0 1 0 1 0 0 1 1 0 1 0 0 1 0 0 1
T_c
Señal transmitida, C = A⊕ B
0 1 1 0 0 1 1 0 0 1 1 0 1 0 1 1 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 0
Receptor
Señal recibida, C
0 1 1 0 0 1 1 0 0 1 1 0 1 0 1 1 1 0 1 0 0 0 1 1 1 0 1 1 0 1 1 0
Secuencia de bits pseudoaleatoria generada localmente, idéntica a B
0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 1 0 1 0 1 0 0 1 1 0 1 0 0 1 0 0 1
Datos de salida, A = C ⊕ B
0 1 0 0 1 0 1 1

Figura 9.6. Ejemplo de espectro expandido de secuencia directa.

En la Figura 9.6 se muestra un ejemplo. Obsérvese que un bit 1 de información invierte los bits pseudoaleatorios, mientras que un bit de información igual a 0 hace que los bits pseudoaleatorios se transmitan sin ser invertidos. La cadena resultante tendrá la misma velocidad de transmisión que la secuencia original pseudoaleatoria, por lo que tendrá un ancho de banda mayor que la secuencia de información. En el ejemplo, el código de expansión tiene una frecuencia de reloj igual a cuatro veces la velocidad de la información.

DSSS USANDO BPSK

Para ver cómo funciona esta técnica en la práctica, supongamos que se emplea un esquema de modulación BPSK. En lugar de representar los datos binarios con 1 y 0, es más adecuado para nuestros fines utilizar $+1$ y -1 para representar los dos dígitos binarios. En tal caso, una señal BPSK se puede representar como se mostró en la Ecuación (5.6):

$$s_d(t) = A\, d(t) \cos(2\pi f_c t)$$

donde

A = amplitud de la señal.

f_c = frecuencia portadora.

$d(t)$ = función discreta que toma el valor $+1$ durante un intervalo de bit si el bit correspondiente de la secuencia es 1, y el valor -1 durante un intervalo de bit si el bit correspondiente de la secuencia es 0.

Para generar una señal DSSS, se multiplica la señal anterior por $c(t)$, la cual es una secuencia PN que toma los valores $+1$ y -1:

$$s(t) = A\, d(t) c(t) \cos(2\pi f_c t)$$

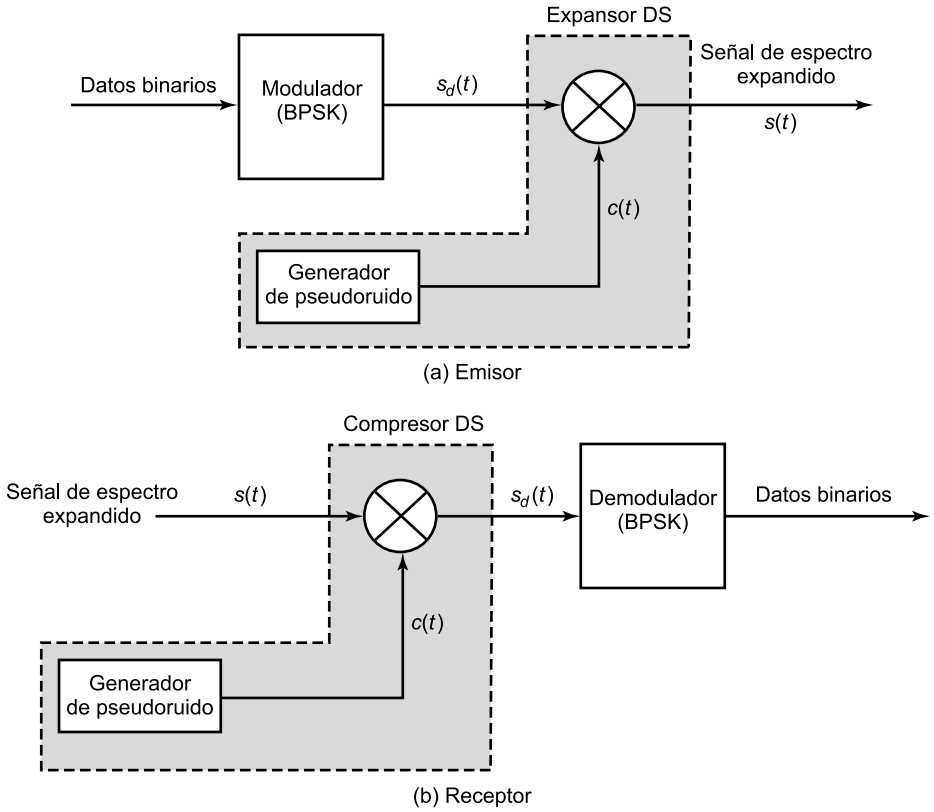


Figura 9.7. Sistema de espectro expandido de secuencia directa.

En el receptor, la señal entrante se multiplica de nuevo por $c(t)$. Dado que $c(t) \times c(t) = 1$, se consigue recuperar la señal original:

$$s(t)c(t) = A\, d(t)c(t)c(t)\cos(2\pi f_c t) = s_d(t)$$

La Ecuación (9.5) puede tener una doble interpretación, dando lugar a dos implementaciones distintas. La primera interpretación consiste en multiplicar $d(t)$ por $c(t)$ y después realizar una modulación BPSK. Ésta es la interpretación que aquí hemos presentado. Frente a ésta, en primer lugar se puede llevar a cabo una modulación BPSK sobre la secuencia de datos $d(t)$ para generar la señal de datos $s_d(t)$, señal que se multiplicará posteriormente por $c(t)$.

En la Figura 9.7 se muestra una implementación haciendo uso de la segunda interpretación. Por su parte, en la Figura 9.8 se ilustra un ejemplo de dicho esquema.

ANÁLISIS DE PRESTACIONES DE DSSS

La expansión del espectro conseguida mediante la técnica de secuencia directa se determina fácilmente (*véase* la Figura 9.9). En nuestro ejemplo, la señal de información tiene una anchura de bit igual a T, lo que equivale a una velocidad igual a $1/T$. En tal caso, el espectro de la señal, dependiendo de la técnica de codificación, es aproximadamente igual a $2/T$. De forma análoga, el espec-

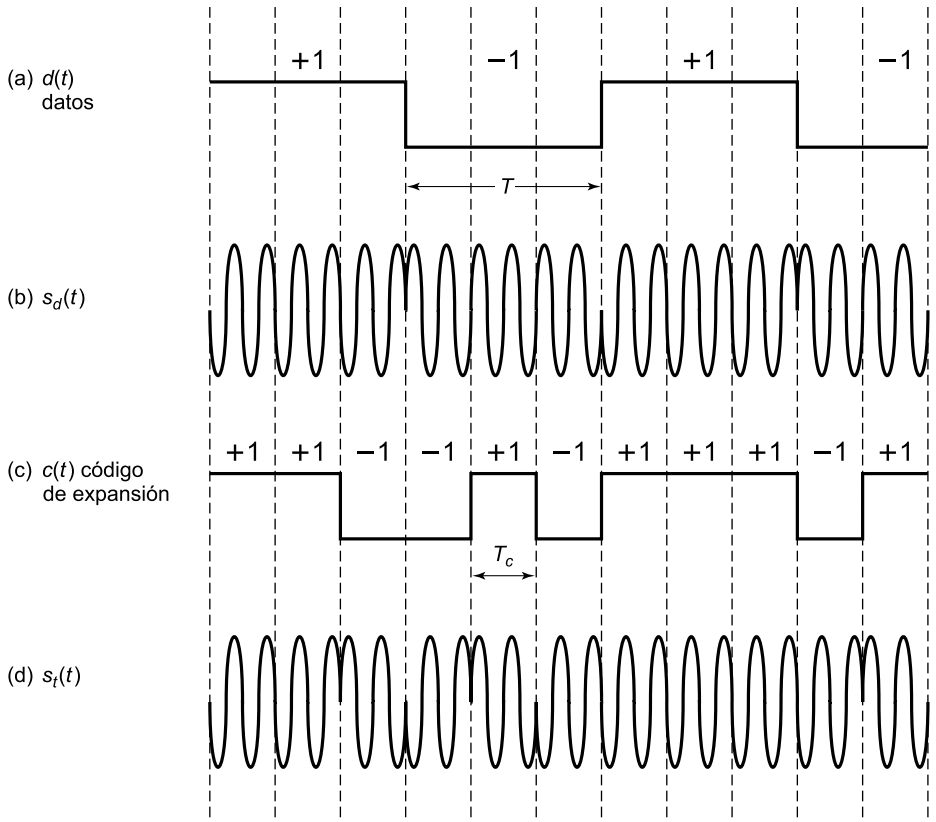


Figura 9.8. Ejemplo de espectro expandido de secuencia directa usando BPSK.

tro de la señal PN es $2/T_c$. La Figura 9.9c muestra la expansión resultante para el espectro, expansión obtenida como resultado directo de la velocidad de la secuencia PN.

Como en el caso FHSS, se pueden estudiar las prestaciones de DSSS en base a su efectividad frente a las interferencias. Supóngase una señal de interferencia sencilla en la frecuencia central del sistema DSSS. Dicha señal de interferencia tiene la forma

$$s_j(t) = \sqrt{2S_j}\cos(2\pi f_c t)$$

y la señal recibida es

$$s_r(t) = s(t) + s_j(t) + n(t)$$

donde

$s(t)$ = señal transmitida.
$s_j(t)$ = señal de interferencia.
$n(t)$ = ruido blanco aditivo.
S_j = potencia de la señal interferente.

El compresor en el receptor multiplica $s_r(t)$ por $c(t)$, de modo que la componente de señal debida a la señal de interferencia es

$$y_j(t) = \sqrt{2S_j}c(t)\cos(2\pi f_c t)$$

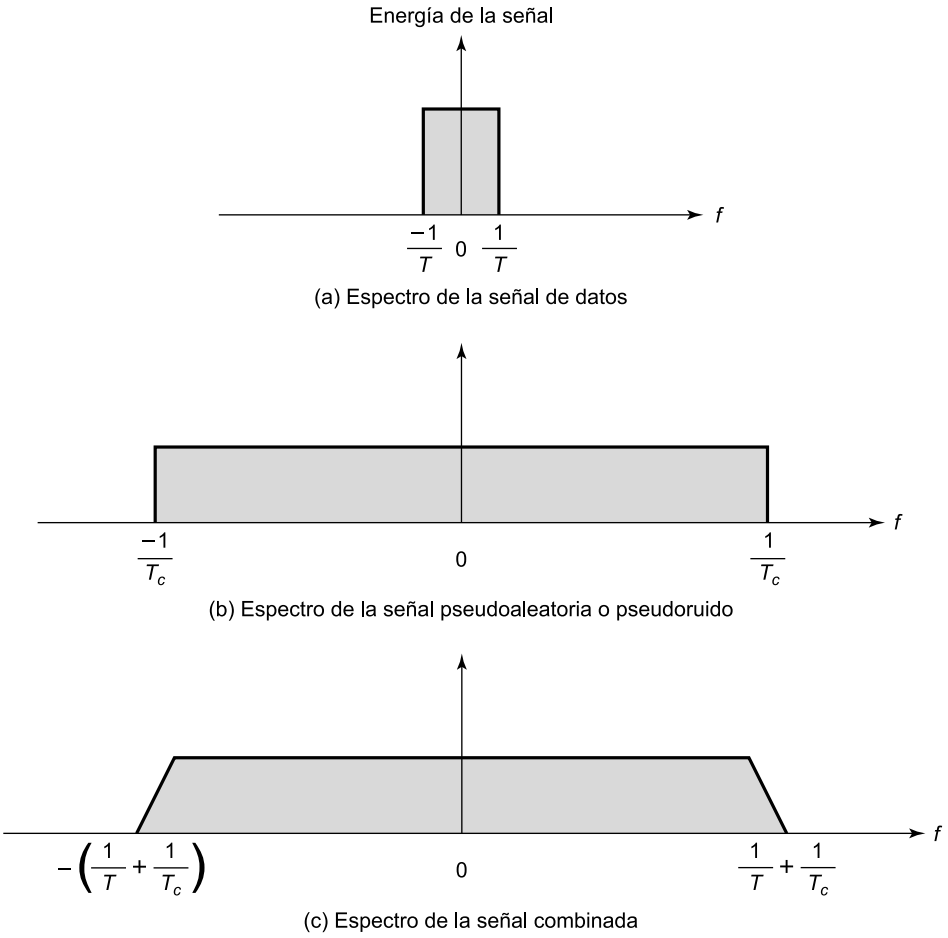


Figura 9.9. Espectro aproximado de una señal de espectro expandido de secuencia directa.

Esto no es más que una modulación BPSK del tono portador. Así, la potencia portadora S_j se expande sobre un ancho de banda de, aproximadamente, $2/T_c$. Sin embargo, el modulador BPSK (*véase* Figura 9.7) que sigue al compresor DSSS incluye un filtro paso-banda destinado a los datos BPSK, con ancho de banda $2/T$. De este modo, la mayor parte de la potencia de la interferencia queda filtrada. Aunque intervienen varios factores, podemos decir que, aproximadamente, la potencia de la interferencia que pasa el filtro es

$$S_{jF} = S_j(2/T)/(2/T_c) = S_j(T_c/T)$$

La potencia interferente queda reducida en un factor (T_c/T) gracias al empleo del esquema de espectro expandido. El inverso de este factor es la ganancia en la relación señal-ruido:

$$G_p = \frac{T}{T_c} = \frac{R_c}{R} \approx \frac{W_s}{W_d}$$

donde R_c es la tasa de expansión de bit, R la velocidad de datos, W_d el ancho de banda de la señal y W_s el ancho de banda de la señal de espectro expandido. El resultado es similar al obtenido para FHSS [Ecuación (9.3)].

9.4. ACCESO MÚLTIPLE POR DIVISIÓN DE CÓDIGO

PRINCIPIOS BÁSICOS

CDMA es una técnica de multiplexación usada con el esquema de espectro expandido y que funciona como sigue. Supongamos una señal de datos de velocidad D, a la que llamaremos velocidad de bits. Se divide cada bit de la secuencia en k minibits («chips») de acuerdo a un patrón fijo específico para cada usuario, denominado código de usuario. El nuevo canal así obtenido tendrá una tasa de minibits igual a kD minibits/segundo. Para ilustrar esto, pensemos en un ejemplo[5] sencillo con $k = 6$. Es sumamente simple caracterizar un código como una secuencia de valores 1 y -1. En la Figura 9.10 se muestran los códigos correspondientes a tres usuarios, A, B y C, cada uno de los cuales se está comunicando con la misma estación base receptora, R. Así, el código para el usuario A es $c_A = \langle 1, -1, -1, 1, -1, 1\rangle$. De forma análoga, el usuario B tiene el código $c_B = \langle 1, 1, -1, -1, 1, 1\rangle$, y el usuario C el código $c_C = \langle 1, 1, -1, 1, 1, -1\rangle$.

Veamos la comunicación del usuario A con la estación base, de la cual se supone que conoce el código de A. Además, supondremos que la comunicación está siempre sincronizada, de modo que la estación base sabe cuándo se reciben datos. Si A desea enviar un bit 1, transmite su código como un patrón de minibits $\langle 1, -1, -1, 1, -1, 1\rangle$. Si se envía un 0, A transmite el complemento (los valores 1 y -1 se invierten) de su código: $\langle -1, 1, 1, -1, 1, -1\rangle$. El receptor en la estación base decodifica el patrón de minibits. En el caso que nos ocupa, el receptor R recibe un patrón de minibits $d = \langle d1, d2, d3, d4, d5, d6\rangle$ y trata de comunicarse con un usuario u del que conoce su

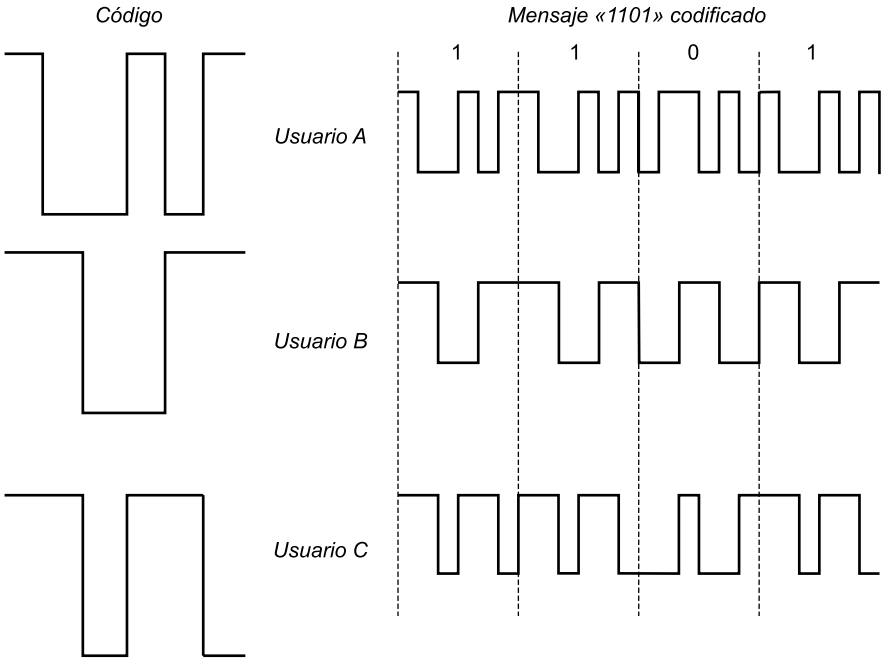


Figura 9.10. Ejemplo de CDMA.

[5] Este ejemplo fue propuesto por el profesor Richard Van Slyke, de la Universidad Politécnica de Brooklyn.

código, $\langle c1, c2, c3, c4, c5, c6\rangle$, llevando a cabo electrónicamente la siguiente función de decodificación:

$$S_u(d) = d1 \times c1 + d2 \times c2 + d3 \times c3 + d4 \times c4 + d5 \times c5 + d6 \times c6$$

El subíndice u de S indica simplemente que u es el usuario en el que estamos interesados. Supongamos que u es A y veamos qué ocurre. Si A envía un bit 1, d será $\langle 1, -1, -1, 1, -1, 1\rangle$ y el cálculo anterior, usando S_A, será

$$S_A(1, -1, -1, 1, -1, 1) = 1 \times 1 + (-1) \times (-1) + (-1) \times (-1) + 1 \times 1 + (-1) \times (-1) + \\ + 1 \times 1 = 6$$

Si A enviase un bit 0, que corresponde a $d = \langle -1, 1, 1, -1, 1, -1\rangle$, se tendría

$$S_A(-1, 1, 1, -1, 1, -1) = -1 \times 1 + 1 \times (-1) + 1 \times (-1) + (-1) \times 1 + 1 \times (-1) + \\ + (-1) \times 1 = -6$$

Obsérvese que siempre se cumple $-6 \leqslant S_A(d) \leqslant = 6$, independientemente de la secuencia de valores -1 y 1 de que conste d, y que los valores extremos 6 y -6 corresponden, respectivamente, al código de A y a su complemento. Por tanto, si S_A vale $+6$, diremos que se ha recibido un 1 de A; si S_A vale -6, diremos que se ha recibido un bit 0 de A; en otro caso, se concluirá que algún otro usuario está enviando información o que se ha producido un error. Entonces, ¿por qué todo esto? La razón es evidente si observamos qué ocurre si el usuario B está transmitiendo y tratamos de recibir haciendo uso de S_A, es decir, si usamos un código erróneo, el de A. Si B envía un bit 1, entonces $d = \langle 1, 1, -1, -1, 1, 1\rangle$, por lo que

$$S_A(1, 1, -1, -1, 1, 1) = 1 \times 1 + 1 \times (-1) + (-1) \times (-1) + (-1) \times 1 + 1 \times (-1) + 1 \times 1 = 0$$

Es decir, la señal no deseada (de B) no se detecta en absoluto. Puede comprobarse fácilmente que si B envía un bit 0, el decodificador obtendrá de nuevo un valor 0 para S_A. Esto significa que si el decodificador es lineal y si A y B transmiten señales s_A y s_B, respectivamente, de forma simultánea, entonces $S_A(s_A + s_B) = S_A(s_A) + S_A(s_B) = S_A(s_A)$, puesto que el decodificador ignora a B cuando utiliza el código de A. Los códigos de A y de B, que presentan la propiedad de que $S_A(c_B) = S_B(c_A) = 0$, se denominan *ortogonales*. Este tipo de códigos son deseables, aunque son escasos los existentes. En este sentido, es más usual el caso en que $S_X(c_Y)$ es pequeño en valor absoluto cuando $X \neq Y$. Así pues, resulta fácil distinguir entre los casos $X = Y$ y $X \neq Y$. En el ejemplo que nos ocupa, $S_A(c_C) = S_C(s_A) = 0$, pero $S_B(c_C) = S_C(c_B) = 2$. En el último caso, la señal C contribuiría un poco, en vez de nada, a la señal decodificada. Utilizando el decodificador, S_u, el receptor puede detectar las transmisiones de u incluso cuando existan otros usuarios emitiendo en la misma celda.

En la Tabla 9.1 se resume el ejemplo de la discusión anterior.

En la práctica, el receptor CDMA puede filtrar la contribución de usuarios no deseados o que aparecen como un ligero ruido de fondo. Sin embargo, si existen varios usuarios compitiendo por conseguir el acceso al canal con el usuario al que desea escuchar el receptor, o si la potencia de una o más de estas señales competidoras es demasiado alta (quizá porque está muy cerca del receptor, problema conocido como «cerca-lejos»), el sistema no funciona adecuadamente.

Tabla 9.1. Ejemplo de CDMA.

a) Códigos de usuario

Usuario A	1	−1	−1	1	−1	1
Usuario B	1	1	−1	−1	1	1
Usuario C	1	1	−1	1	1	−1

b) Transmisión desde A

Transmisión (bit = 1)	1	−1	−1	1	−1	1	
Palabra recibida	1	−1	−1	1	−1	1	
Multiplicación	1	1	1	1	1	1	= 6

Transmisión (bit = 0)	−1	1	1	−1	1	−1	
Palabra recibida	1	−1	−1	1	−1	1	
Multiplicación	−1	−1	−1	−1	−1	−1	= 6

c) Transmisión desde B, el receptor intenta recuperar la transmisión de A

Transmisión (bit = 1)	1	1	−1	−1	1	1	
Palabra recibida	1	−1	−1	1	−1	1	
Multiplicación	1	−1	1	−1	−1	1	= 0

d) Transmisión desde C, el receptor intenta recuperar la transmisión de B

Transmisión (bit = 1)	1	1	−1	1	1	−1	
Palabra recibida	1	1	−1	−1	1	1	
Multiplicación	1	1	1	−1	1	−1	= 2

e) Transmisión desde B y desde C, el receptor intenta recuperar la transmisión de B

B (bit = 1)	1	1	−1	−1	1	1	
C (bit = 1)	1	1	−1	1	1	−1	
Señal combinada	2	2	−2	0	2	0	
Palabra recibida	1	1	−1	−1	1	1	
Multiplicación	2	2	2	0	2	0	= 8

CDMA PARA ESPECTRO EXPANDIDO DE SECUENCIA DIRECTA

Estudiemos ahora CDMA desde el punto de vista de un sistema DSSS que hace uso de BPSK. En la Figura 9.11 se muestra una configuración en la que existen n usuarios, cada uno de ellos transmitiendo y haciendo uso de una secuencia PN diferente ortogonal (compárese con la Figura 9.7).

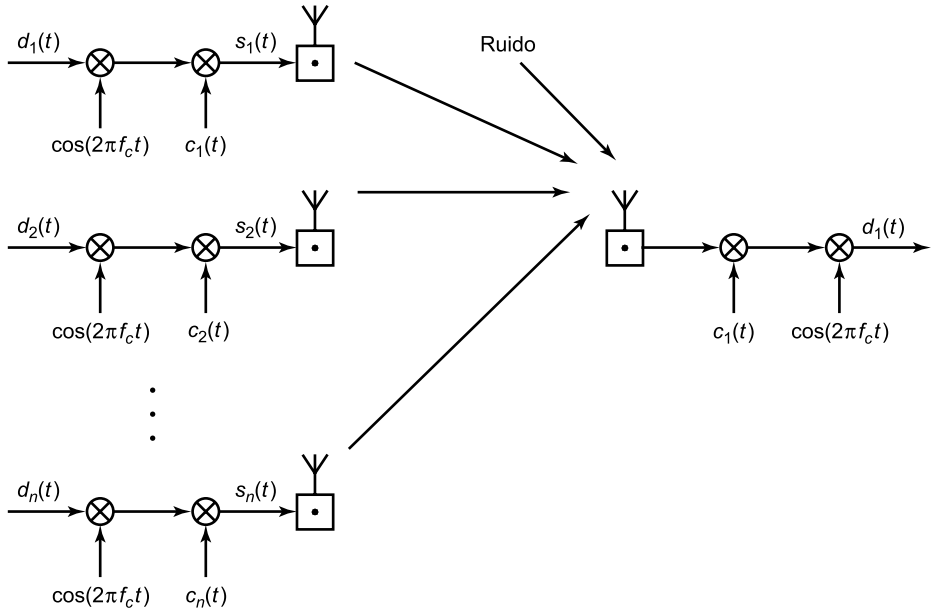


Figura 9.11. CDMA en un entorno DSSS.

Para cada uno de los usuarios, la secuencia de datos a transmitir, $d_i(t)$, se modula BPSK para obtener una señal de ancho de banda W_s y, tras ello, se multiplica por el código de expansión de dicho usuario, $c_i(t)$. Todas las señales, además de ruido, se reciben en la antena del receptor. Supóngase que éste trata de recuperar los datos del usuario 1. Para ello, multiplica la señal entrante por el código expansor de dicho usuario y, a continuación, demodula. El efecto de este proceso es la compresión del ancho de banda de aquella parte de la señal entrante correspondiente al usuario 1 al ancho de banda original de la señal no expandida, el cual es proporcional a la velocidad de los datos. Puesto que el resto de la señal entrante es ortogonal al código expansor del usuario 1, dicho resto de señal seguirá teniendo un ancho de banda W_s. Así pues, la energía de la señal no deseada permanece distribuida en un ancho de banda grande, mientras que la de la señal deseada se concentra en un ancho de banda estrecho. El filtro paso-banda en el demodulador puede, en consecuencia, recuperar la señal deseada.

9.5. LECTURAS RECOMENDADAS

Tanto [PETE95] como [DIXO94] ofrecen un buen estudio acerca del esquema de espectro expandido. [TANT98] contiene una reedición de artículos importantes en este campo, entre los que se encuentra [PICK82], el cual proporciona una excelente introducción al espectro expandido.

DIXO94 Dixon, R. *Spread Spectrum Systems with Commercial Applications*. New York: Wiley, 1994.

PETE95 Peterson, R.; Ziemer, R.; y Borth, D. *Introduction to Spread Spectrum Communications*. Englewood Cliffs, NJ: Prentice Hall, 1995.

PICK82 Pickholtz, R.; Schilling, D.; y Milstein, L. «Theory of Spread Spectrum Communications—A Tutorial.» *IEEE Transactions on Communications*, mayo 1982. Reeditado en [TANT98].

TANT98 Tantaratana, S. y Ahmed, K., eds. *Wireless Applications of Spread Spectrum Systems*: *Selected Readings*. Piscataway, NJ: IEEE Press, 1998.

9.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

acceso múltiple por división de código (CDMA)
código expansor
espectro expandido
espectro expandido de secuencia directa (DSSS)
espectro expandido por salto de frecuencias (FHSS)
FHSS lento
FHSS rápido
minibit («chip»)
ortogonal
secuencia de expansión
pseudoruido (PN)

CUESTIONES DE REPASO

9.1. ¿Cuál es la relación entre el ancho de banda de una señal antes y después de su codificación mediante el esquema de espectro expandido?

9.2. Enumere tres ventajas del esquema de espectro expandido.

9.3. ¿Qué es el espectro expandido por salto de frecuencias?

9.4. Explique la diferencia entre FHSS lento y FHSS rápido.

9.5. ¿Qué es el espectro expandido de secuencia directa?

9.6. ¿Cuál es la relación entre la velocidad de una señal antes y después de su codificación mediante el esquema DSSS?

9.7. ¿Qué es CDMA?

EJERCICIOS

9.1. Suponga que se desea transmitir una secuencia de datos a 56 kbps usando el esquema de espectro expandido:

a) Calcule el ancho de banda necesario para ello en los casos SNR = 0,1, 0,01 y 0,001.

b) En un sistema normal (no espectro expandido) resulta razonable la consecución de una eficiencia del ancho de banda en torno a 1 bps/Hz. Es decir, para transmitir una secuencia de datos de 56 kbps se emplea un ancho de banda de 56 kHz. En tal caso, ¿cuál será la SNR mínima que garantiza dicha transmisión sin la ocurrencia de errores apreciables? Compare el resultado con el caso de usar espectro expandido.

Sugerencia: revise el estudio de la capacidad de canal visto en la Sección 3.4.

9.2. Un sistema FHSS utiliza un ancho de banda total de $W_s = 400$ MHz y un ancho de banda por canal de 100 Hz. ¿Cuál es el número mínimo de bits PN necesarios para cada salto de frecuencia?

9.3. Un sistema FHSS que usa MFSK con $M = 4$ considera 1.000 frecuencias diferentes. ¿Cuál es la ganancia de procesamiento?

9.4. En la siguiente tabla se ilustra el funcionamiento de un sistema FHSS durante un periodo completo de la secuencia PN.

Tiempo	0	1	2	3	4	5	6	7	8	9	10	11
Datos de entrada	0	1	1	1	1	1	1	0	0	0	1	0
Frecuencia	f_1		f_3		f_{27}		f_{26}		f_8		f_{10}	
Secuencia PN	001				110				011			

Tiempo	12	13	14	15	16	17	18	19
Datos de entrada	0	1	1	1	1	0	1	0
Frecuencia	f_1		f_3		f_2		f_2	
Secuencia PN	001				001			

a) ¿Cuál es el periodo de la secuencia PN?

b) El sistema utiliza una variante de FSK, ¿cuál es ésta?

c) ¿Cuál es el número de bits por símbolo?

d) ¿Cuál es el número de frecuencias FSK?

e) ¿Cuál es la longitud de una secuencia PN por salto?

f) ¿Es un sistema FH lento o rápido?

g) ¿Cuál es el número total de saltos posibles?

h) Muestre la variación de la frecuencia de salto a lo largo del tiempo.

9.5. La tabla siguiente ilustra el funcionamiento de un sistema FHSS que utiliza la misma secuencia PN que la del Ejercicio 4.

Tiempo	0	1	2	3	4	5	6	7	8	9	10	11
Datos de entrada	0	1	1	1	1	1	1	0	0	0	1	0
Frecuencia	f_1	f_{21}	f_{11}	f_3	f_3	f_3	f_{22}	f_{10}	f_0	f_0	f_2	f_{22}
Secuencia PN	001	110	011	001	001	001	110	011	001	001	001	110

Tiempo	12	13	14	15	16	17	18	19
Datos de entrada	0	1	1	1	1	0	1	0
Frecuencia	f_9	f_1	f_3	f_3	f_{22}	f_{10}	f_2	f_2
Secuencia PN	011	001	001	001	110	011	001	001

a) ¿Cuál es el periodo de la secuencia PN?

b) El sistema utiliza una variante de FSK, ¿cuál es ésta?

c) ¿Cuál es el número de bits por símbolo?

d) ¿Cuál es el número de frecuencias FSK?

e) ¿Cuál es la longitud de una secuencia PN por salto?

f) ¿Se trata de un sistema FH lento o de uno rápido?

g) ¿Cuál es el número total de saltos posibles?

h) Muestre la variación de la frecuencia de salto a lo largo del tiempo.

9.6. Considere un esquema MSK con $f_c = 250$ kHz, $f_d = 25$ kHz y $M = 8$ ($L = 3$ bits).

a) Haga una asignación de frecuencias para cada una de las ocho posibles combinaciones de 3 bits.

b) Se desea aplicar FHSS a este esquema MSK con $k = 2$; es decir, el sistema saltará entre cuatro frecuencias posibles. Extienda el resultado de la parte (a) para mostrar las $4 \times 8 = 32$ asignaciones de frecuencia.

9.7. En la Figura 9.12, basada en una de [BELL00], se muestra un esquema simplificado de codificación y decodificación CDMA. Existen siete canales lógicos, todos ellos usando un esquema DSSS con un código expansor de 7 bits. Suponga que todas las fuentes están sincronizadas. Si las siete fuentes transmiten un bit de datos, en forma de una secuencia de 7 bits, todas las señales se combinan en el receptor de modo que dos valores positivos o dos negativos se refuerzan, mientras que uno positivo y uno negativo se cancelan. Para decodificar un canal dado, el receptor multiplica la señal compuesta entrante por el código de expansión de dicho canal, suma el resultado y asigna un 1 binario a un valor positivo y un 0 binario a un valor negativo.

a) ¿Cuáles son los códigos de expansión para los siete canales?

b) Determine la salida dada por el receptor para el canal 1 y el valor binario asignado.

c) Repita la parte (b) para el canal 2.

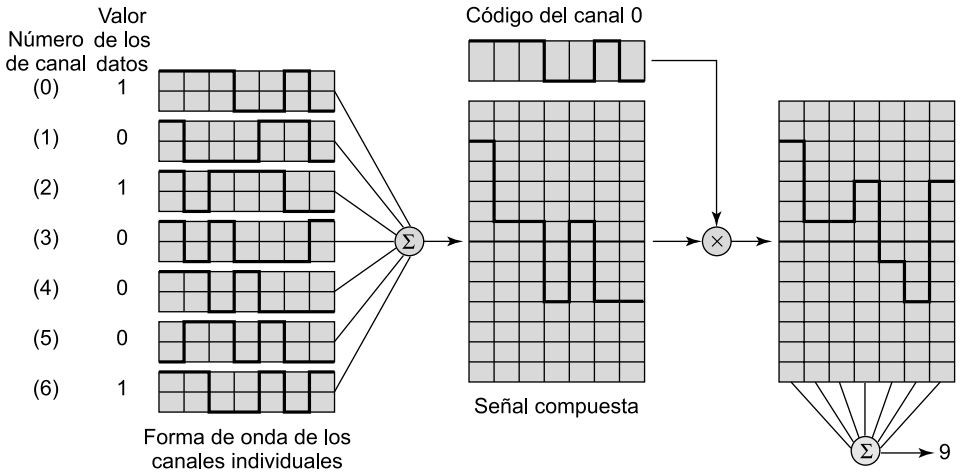


Figura 9.12. Ejemplo de codificación y decodificación CDMA de siete canales.

9.8. Con diferencia, la técnica más ampliamente usada para la generación de números pseudoaleatorios es el método lineal congruente. El algoritmo se parametriza a través de los siguientes cuatro números:

m el módulo, $m > 0$

a el multiplicador, $0 \leqslant a < m$

c el incremento, $0 \leqslant c < m$

X_0 el valor inicial, o semilla, $0 \leqslant X_0 < m$

La secuencia de números pseudoaleatorios $\{X_n\}$ se obtiene mediante la siguiente ecuación iterativa:

$$X_{n+1} = (aX_n + c) \bmod m$$

Si m, a, c y X_0 son enteros, esta técnica producirá una secuencia de números enteros, cada uno de ellos en el rango $0 = X_n < m$. Una característica fundamental de un generador de números pseudoaleatorios es que la secuencia generada parece aleatoria. Aunque no lo es, puesto que se genera de forma determinista, existen varios tests estadísticos que pueden usarse para determinar el grado de aleatoriedad de la misma. Otra característica deseable es que la función debería ser generadora de periodo completo, es decir, debería generar todos los números entre 0 y m antes de repetir valores.

Con el algoritmo lineal congruente, la elección de parámetros que permite un periodo completo no garantiza necesariamente una buena aleatorización. Considérense, por ejemplo, los dos siguientes generadores:

$$X_{n+1} = (6X_n) \bmod 13$$
$$X_{n+1} = (7X_n) \bmod 13$$

Escriba las dos secuencias para mostrar que ambas son de periodo completo. ¿Cuál le parece más aleatoria de las dos?

9.9. Sería deseable que m fuese muy elevado a fin de poder generar varias series de números aleatorios distintas. Un criterio usual es que m sea aproximadamente igual al máximo entero no negativo representable por un computador. Así, generalmente se considera un valor de m próximo a 2^{31}. Muchos expertos recomiendan un valor de $2^{31} - 1$. Puede resultar extraño no usar sencillamente 2^{31}, ya que este número puede representarse sin bits adicionales, además del hecho de que la operación módulo resulta más fácil. En general, se prefiere el módulo $2^k - 1$ al 2^k. ¿Por qué?

9.10. Cualquiera que sea el uso de números pseudoaleatorios, sea para cifrado, simulación o diseño estadístico, es peligroso confiar ciegamente en el generador de números aleatorios existente en la librería del sistema de su computador. [PARK88] constató que muchos textos y paquetes de programación actuales utilizan algoritmos erróneos para la generación de números aleatorios. Este ejercicio va a ayudar a testar su sistema.

El test se basa en un teorema atribuido a Ernesto Cesaro (*véase* [KNUT98] para su demostración), el cual establece que la probabilidad de que el máximo común divisor de dos números enteros elegidos aleatoriamente sea 1 es igual a $\frac{6}{\pi^2}$. Use este teorema en un programa para determinar estadísticamente el valor de π. El programa principal debe llamar a

tres subprogramas: el generador de números aleatorios que, a partir de la librería del sistema, genere los enteros aleatorios; un subprograma que calcule el máximo común divisor de dos números enteros utilizando el algoritmo de Euclides; y un subprograma que calcule la raíz cuadrada de un número. Puede que tenga que escribir los dos últimos programas mencionados. El programa principal debe procesar una gran cantidad de números aleatorios para obtener una estimación de la probabilidad anteriormente mencionada. A partir de ella, resulta sencillo estimar el valor de π.

Si el resultado está próximo a 3,14, ¡enhorabuena! Si no es así, el resultado obtenido es probablemente pequeño, generalmente en torno a 2,7. ¿A qué se debe la obtención de un resultado tan pequeño?

PARTE III

REDES DE ÁREA AMPLIA

CUESTIONES DE LA PARTE III

En la Parte II del texto se ha abordado el estudio de la transferencia de datos entre dispositivos directamente conectados, generalmente mediante un enlace punto a punto. Sin embargo, tal disposición resulta impracticable en ocasiones, siendo necesaria la existencia de una red de comunicación para la transmisión de los datos entre los dispositivos; bien porque éstos se encuentran geográficamente muy alejados, o bien porque existen varios dispositivos a interconectar. En general, las redes de comunicación se pueden clasificar como de área amplia (WAN) o de área local (LAN), centrándose la Parte III del texto en el estudio de las redes WAN y la Parte IV en el de las LAN.

Existen dos cuestiones importantes a destacar en relación al estudio de la interconexión de redes abordado en la Parte V del libro. En primer lugar, las redes constitutivas de Internet y otras redes de este tipo son LAN y WAN, por lo que la comprensión de la tecnología y de la arquitectura de las redes internet implica la comprensión de las redes subyacentes en que se basan. En segundo lugar, y quizá más importante, hay que señalar que muchas de las tecnologías desarrolladas para WAN conmutadas (incluyendo la conmutación de paquetes, la retransmisión de tramas y las redes ATM) forman parte del diseño de la interconexión de redes. Esto es especialmente cierto por lo que respecta al encaminamiento y al control de congestión.

ESTRUCTURA DE LA PARTE III

CAPÍTULO 10. CONMUTACIÓN DE CIRCUITOS Y DE PAQUETES

El estudio planteado en este tema acerca de la tecnología y arquitectura de las redes de conmutación de circuitos comienza con el funcionamiento interno de un conmutador simple. Por el contrario, las redes de conmutación de paquetes se introducen mejor a partir del comportamiento del conjunto de conmutadores que constituyen la red. De este modo, el Capítulo 10 comienza examinando los conceptos de conmutación digital, entre los que se encuentran los de conmutación por división en el espacio y en el tiempo. Tras ello, se discuten las cuestiones relacionadas con una red de conmutación de circuitos multinodal, centrando la atención en aspectos de señalización.

A lo largo del resto del Capítulo 10 se presenta la tecnología de conmutación de paquetes, abordando cuestiones fundamentales relativas a esta tecnología y llevando a cabo el análisis de los esquemas de datagramas y de circuitos virtuales. Adicionalmente, el capítulo trata las redes de retransmisión de tramas (*frame relay*).

CAPÍTULO 11. MODO DE TRANSFERENCIA ASÍNCRONO

El Capítulo 11 se centra en la tecnología de transmisión que constituye la base de la RDSI de banda ancha: el modo de transferencia asíncrono (ATM, *Asynchronous Transfer Mode*). ATM encuentra un amplio uso más allá del contexto de RDSI de banda ancha, siendo en su esencia una tecnología de conmutación de paquetes. No obstante este hecho, resulta más funcional y eficiente que la conmutación de paquetes tradicional, estando diseñada para proporcionar velocidades de transmisión muy elevadas. Este capítulo comienza con una descripción del protocolo y formato ATM, tras lo que se discuten aspectos de la capa física en referencia a la transmisión de celdas ATM, así como la capa de adaptación ATM (AAL, *ATM Adaptation Layer*).

CAPÍTULO 12. ENCAMINAMIENTO EN REDES CONMUTADAS

Una cuestión técnica importante relativa a las redes conmutadas es la de encaminamiento. Dado que los nodos origen y destino de una comunicación no están directamente conectados, la red debe encaminar cada paquete nodo a nodo a través de la red. El Capítulo 12 ofrece un breve estudio de aspectos de encaminamiento para redes de conmutación de circuitos, abordándose posteriormente esta misma función para el caso de las redes de conmutación de paquetes.

CAPÍTULO 13. CONTROL DE CONGESTIÓN EN REDES DE DATOS

Un aspecto crítico en el diseño de redes conmutadas es el relativo al control de congestión. Este capítulo comienza con un estudio acerca de la naturaleza de la congestión en redes de datos y de la importancia y dificultad de su control. El Capítulo 13 proporciona una discusión general acerca del control de congestión en redes de conmutación de paquetes tradicionales, así como en redes basadas en retransmisión de tramas. El resto del capítulo se centra en el estudio del control de congestión en redes ATM, uno de los aspectos más complejos de ATM y objeto de investigación intensiva en la actualidad. En este capítulo se presentan aquellas técnicas más ampliamente aceptadas para su utilización en entornos ATM.

CAPÍTULO 14. REDES INALÁMBRICAS CELULARES

El Capítulo 14 comienza con una discusión acerca de cuestiones importantes relacionadas con redes inalámbricas celulares. Seguidamente, el tema presenta el servicio de telefonía móvil tradicional, conocido como primera generación analógica. Tras ello, se examinan las redes celulares digitales de segunda generación y, para concluir, las redes de tercera generación.

CAPÍTULO 10

Conmutación de circuitos y de paquetes

10.1. Redes conmutadas

10.2. Redes de conmutación de circuitos

10.3. Conceptos de conmutación de circuitos
Conmutación por división en el espacio
Conmutación por división en el tiempo

10.4. Señalización de control
Funciones de señalización
Localización de la señalización
Señalización por canal común
Sistema de señalización número 7

10.5. Arquitectura de conmutación lógica

10.6. Principios de conmutación de paquetes
Técnica de conmutación
Tamaño de paquete
Comparación de las técnicas de conmutación de circuitos y de paquetes

10.7. X.25

10.8. Retransmisión de tramas
Fundamentos
Arquitectura de protocolos en retransmisión de tramas
Transferencia de datos de usuario

10.9. Lecturas y sitios web recomendados

10.10. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- La conmutación de circuitos se usa en redes telefónicas públicas y es la base de redes privadas implementadas con líneas alquiladas y que utilizan conmutadores de circuitos *in situ*. La técnica de conmutación de circuitos se desarrolló para tráfico de voz, aunque también puede gestionar tráfico de datos, si bien su uso en este último tipo de aplicaciones resulta ineficiente en ocasiones.
- En la conmutación de circuitos se establece un canal de comunicaciones dedicado entre dos estaciones. Se reservan recursos de transmisión y de conmutación de la red para su uso exclusivo en el circuito durante la conexión. Ésta es transparente: una vez establecida parece como si los dispositivos estuviesen directamente conectados.
- Diversos aspectos importantes de las redes de conmutación de circuitos han cambiado de forma drástica con el incremento de la complejidad y digitalización de las redes de telecomunicaciones públicas. Así, esquemas simples de encaminamiento jerárquico han sido reemplazados por otros no jerárquicos más flexibles y potentes. Esto evidencia el cambio adoptado en la arquitectura subyacente, lo que permite un incremento en la eficiencia y en la flexibilidad. Los métodos de señalización de control intracanal se han reemplazado por técnicas de señalización por canal común más complejas y de mayor velocidad.
- La técnica de conmutación de paquetes se diseñó para ofrecer un servicio más eficiente que el proporcionado por la conmutación de circuitos para el tráfico de datos. En la conmutación de paquetes, una estación realiza la transmisión de los datos en base a pequeños bloques llamados paquetes, cada uno de los cuales contiene una parte de los datos de usuario, además de información de control necesaria para el adecuado funcionamiento de la red.
- Un elemento clave distintivo de las redes de conmutación de paquetes lo constituye el hecho de que el funcionamiento interno puede basarse en datagramas o en circuitos virtuales. En el caso de los circuitos virtuales internos se define una ruta entre dos puntos de comunicación finales o extremos, de modo que todos los paquetes para dicho circuito virtual siguen el mismo camino. Por su parte, en el caso de los datagramas internos, cada paquete se trata de forma independiente, por lo que paquetes con el mismo destino pueden seguir rutas diferentes.
- X.25 es el protocolo estándar para la interfaz entre los sistemas finales y una red de conmutación de paquetes.
- La técnica de retransmisión de tramas (*frame relay*) es una forma de conmutación de paquetes que proporciona una interfaz funcional similar a X.25, con prestaciones mejoradas.

En la Parte II del texto se estudió la forma en que se codifica y transmite la información sobre un enlace de comunicaciones. Ahora nos centraremos en una discusión más general acerca de las redes, las cuales pueden usarse para interconectar varios dispositivos. El capítulo comienza con un estudio general acerca de las redes de comunicación conmutadas, dedicándose el resto del tema a las redes de área amplia y, en particular, a enfoques tradicionales para el diseño de este tipo de redes: conmutación de circuitos y conmutación de paquetes.

La conmutación de circuitos ha sido la tecnología dominante en las comunicaciones de voz desde la invención del teléfono, y así ha seguido siendo con la llegada de la era digital. Este capítulo presenta las características principales de las redes de conmutación de circuitos.

En torno a 1970 se ideó una nueva forma de arquitectura para comunicaciones de datos digitales de larga distancia: la conmutación de paquetes. Aunque la tecnología de esta técnica de conmu-

tación ha evolucionado sustancialmente desde entonces, se ha de reseñar: (1) que la tecnología básica en conmutación de paquetes es esencialmente la misma en la actualidad que la de las redes de principios de los años setenta, y (2) que la conmutación de paquetes continúa siendo una de las pocas tecnologías efectivas para comunicaciones de datos a larga distancia.

En este capítulo se presenta la tecnología de conmutación de paquetes. Se verá que muchas de las ventajas de esta tecnología (flexibilidad, compartición de recursos, robustez, efectividad) conllevan un coste. Una red de conmutación de paquetes es un conjunto distribuido de nodos de conmutación de paquetes, los cuales, idealmente, conocen siempre el estado de la red completa. Desgraciadamente, dado que los nodos se encuentran distribuidos, existe un tiempo de retardo entre la producción de un cambio en el estado de una parte de la red y la constatación de dicho cambio por parte de todos los nodos. Además, existe un coste adicional asociado a la comunicación de la información relativa al estado. En consecuencia, una red de conmutación de paquetes nunca funcionará «perfectamente», utilizándose complicados algoritmos para solventar el retardo temporal y los costes debidos al funcionamiento de la red. Estas mismas cuestiones aparecerán de nuevo cuando estudiemos la interconexión de redes en la Parte V del texto.

Finalmente, el capítulo presenta una forma popular de conmutación de paquetes conocida como retransmisión de tramas (*frame relay*).

10.1. REDES CONMUTADAS

Para la transmisión de datos[1] más allá de un entorno local, la comunicación se realiza normalmente mediante la transmisión de datos desde el origen hasta el destino a través de una red de nodos de conmutación intermedios. Este diseño de red conmutada se usa también a veces para implementar redes LAN. El contenido de los datos no es del interés de los nodos de conmutación, sino que el propósito de estos últimos es proporcionar un servicio de conmutación que posibilite el intercambio de datos entre nodos hasta alcanzar el destino deseado. En la Figura 10.1 se muestra una red sencilla, en la que los dispositivos finales que desean comunicarse se denominan *estaciones*. Éstas pueden ser computadores, terminales, teléfonos u otros dispositivos de comunicación. Por su parte, a los dispositivos de conmutación cuyo objetivo es proporcionar la comunicación se les denomina *nodos*. Los nodos están conectados entre sí mediante enlaces de transmisión, formando una topología dada. Cada estación se conecta a un nodo, llamándose *red de comunicaciones* al conjunto de todos los nodos.

Los tipos de redes estudiados en este capítulo, así como en los tres siguientes, se denominan *redes de comunicación conmutadas*. Los datos que entran a la red procedentes de una estación se encaminan hacia el destino mediante su conmutación de nodo en nodo. Por ejemplo, en la Figura 10.1, los datos desde la estación A con destino a la estación F se envían al nodo 4. Éstos se pueden encaminar hasta el destino a través de los nodos 5 y 6, o bien vía los nodos 7 y 6. Diversas consideraciones se pueden realizar acerca de las redes conmutadas:

1. Algunos nodos sólo se conectan con otros nodos (por ejemplo, los nodos 5 y 7), siendo su única tarea la conmutación interna (en la red) de los datos. Otros nodos tienen también conectadas una o más estaciones, de modo que, además de sus funciones de conmutación, estos nodos aceptan datos desde y hacia las estaciones conectadas a ellos.

[1] Este término se usa aquí en un sentido muy general para referirnos a voz, imágenes y vídeo, así como datos ordinarios (datos numéricos o texto, por ejemplo).

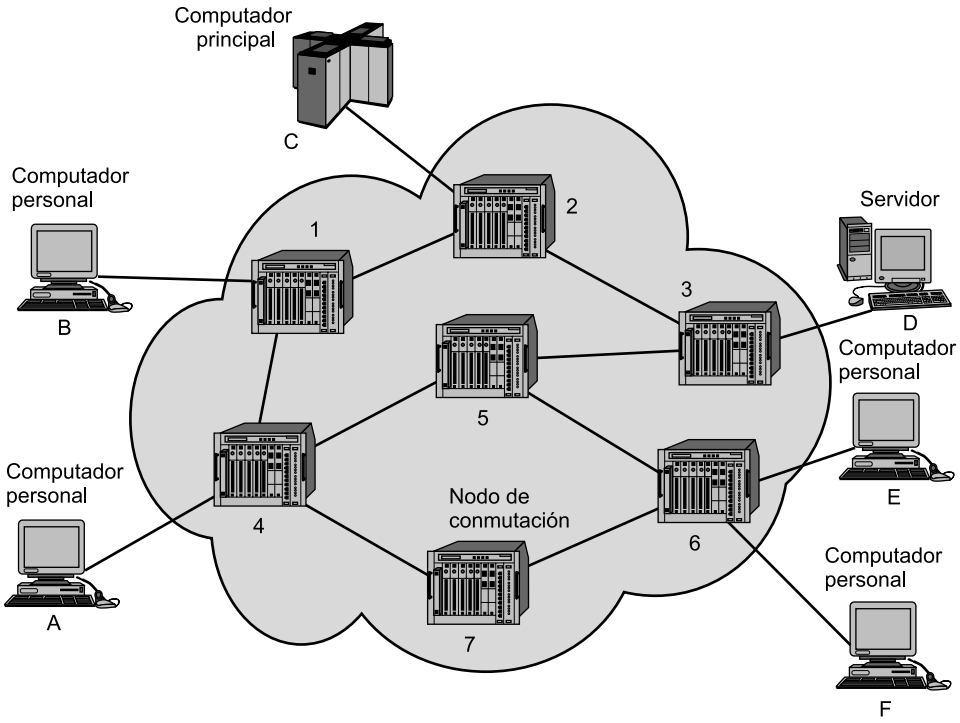


Figura 10.1. Red de conmutación simple.

2. Los enlaces entre nodos están normalmente multiplexados, utilizándose multiplexación por división en frecuencias (FDM) o por división en el tiempo (TDM).
3. Por lo general, la red no está completamente conectada; es decir, no existe un enlace directo entre cada posible pareja de nodos. Sin embargo, siempre resulta deseable tener más de un camino posible a través de la red para cada par de estaciones. Esto mejora la fiabilidad o seguridad de la red.

En las redes conmutadas de área amplia se emplean dos tecnologías diferentes: conmutación de circuitos y conmutación de paquetes. Estas dos tecnologías difieren en la forma en que los nodos conmutan la información entre enlaces en el camino desde el origen hasta el destino.

10.2. REDES DE CONMUTACIÓN DE CIRCUITOS

Las comunicaciones mediante la conmutación de circuitos implican la existencia de un camino o canal de comunicación dedicado entre dos estaciones, el cual consiste en una secuencia de enlaces conectados entre nodos de la red. En cada uno de los enlaces físicos se dedica un canal lógico para cada conexión establecida. La comunicación vía la conmutación de circuitos implica tres fases, que se pueden explicar haciendo referencia a la Figura 10.1.

1. **Establecimiento del circuito.** Antes de transmitir señal alguna, se debe establecer un circuito extremo a extremo (estación a estación). Por ejemplo, la estación A envía una solicitud al nodo 4 pidiendo una conexión con la estación E. Generalmente, el enlace entre A y

4 es una línea dedicada, por lo que esa parte de la conexión existe ya. El nodo 4 debe encontrar el siguiente enlace de la ruta para alcanzar el nodo 6. En función de la información de encaminamiento y de las medidas de disponibilidad y, quizá, del coste, el nodo 4 selecciona el enlace hacia el nodo 5, reserva un canal libre del enlace (utilizando FDM o TDM) y envía un mensaje a E solicitando la conexión. Tras esto queda establecido un camino dedicado desde A hasta 5 a través de 4. Dado que pueden existir varias estaciones conectadas al nodo 4, éste debe ser capaz de establecer rutas internas desde varias estaciones a múltiples nodos. El resto del proceso es similar. El nodo 5 reserva un canal hasta el nodo 6 y asigna internamente este canal al que viene desde el nodo 4. El nodo 6 completa la conexión con E, para lo cual se realiza un test con objeto de determinar si E está ocupada o, por el contrario, se encuentra lista para aceptar la conexión.

2. **Transferencia de datos.** Tras el establecimiento del circuito se puede transmitir la información desde A hasta E a través de la red. Los datos pueden ser analógicos o digitales, dependiendo de la naturaleza de la red. Debido a la tendencia actual de migración hacia redes digitales completamente integradas, la utilización de transmisiones digitales (binarias) tanto de voz como de datos se está convirtiendo en el método de comunicaciones predominante. El camino del ejemplo está constituido por el enlace A-4 (conmutación interna a través de 4), el canal 4-5 (conmutación interna a través de 5), el canal 5-6 (conmutación interna a través de 6) y el enlace 6-E. Normalmente, la conexión es *full-duplex*.

3. **Desconexión del circuito.** Tras la fase de transferencia de datos, la conexión finaliza por orden de una de las dos estaciones involucradas. Las señales se deben propagar a los nodos 4, 5 y 6 para que éstos liberen los recursos dedicados a la conexión que se cierra.

Obsérvese que el canal de conexión se establece antes de que comience la transmisión de datos, por lo que la capacidad del canal se debe reservar entre cada par de nodos en la ruta y cada nodo debe ser capaz de conmutar internamente para gestionar la conexión solicitada. En definitiva, los conmutadores deben contar con la inteligencia necesaria para realizar estas reservas y establecer una ruta a través de la red.

La conmutación de circuitos puede llegar a ser bastante ineficiente. La capacidad del canal se dedica permanentemente a la conexión mientras dura ésta, incluso si no se transfieren datos. Aunque no se alcanza el 100 por cien, la utilización puede ser bastante alta para una conexión de voz. Por su parte, para comunicaciones entre un terminal y un computador, es posible que el canal esté libre durante la mayor parte de la conexión. Desde el punto de vista de las prestaciones, existe un retardo previo a la transferencia de las señales debido al establecimiento de la llamada; no obstante, una vez establecido el circuito, la red es transparente para los usuarios. La información se transmite a una velocidad fija sin otro retardo que el de propagación a través de los enlaces de transmisión, siendo despreciable el retardo introducido por cada nodo de la ruta.

La conmutación de circuitos fue desarrollada para el tráfico de voz, pero en la actualidad se usa también para el tráfico de datos. El mejor ejemplo conocido de una red de conmutación de circuitos es el de la red telefónica pública (*véase* Figura 10.2), la cual es en la actualidad un conjunto de redes nacionales interconectadas para ofrecer un servicio internacional. Aunque fue ideada e implementada inicialmente para ofrecer un servicio de telefonía analógica a los abonados, en la actualidad opera con una gran cantidad de tráfico de datos vía módem y está siendo convertida progresivamente en una red digital. Otra aplicación bien conocida de la conmutación de circuitos son las centralitas privadas (PBX, *Private Branch eXchange*), usadas para conectar los teléfonos dentro de un edificio u oficina. También se utiliza la conmutación de circuitos en redes privadas. Este tipo de redes se utiliza usualmente en compañías u organizaciones para conectar sus diferentes delega-

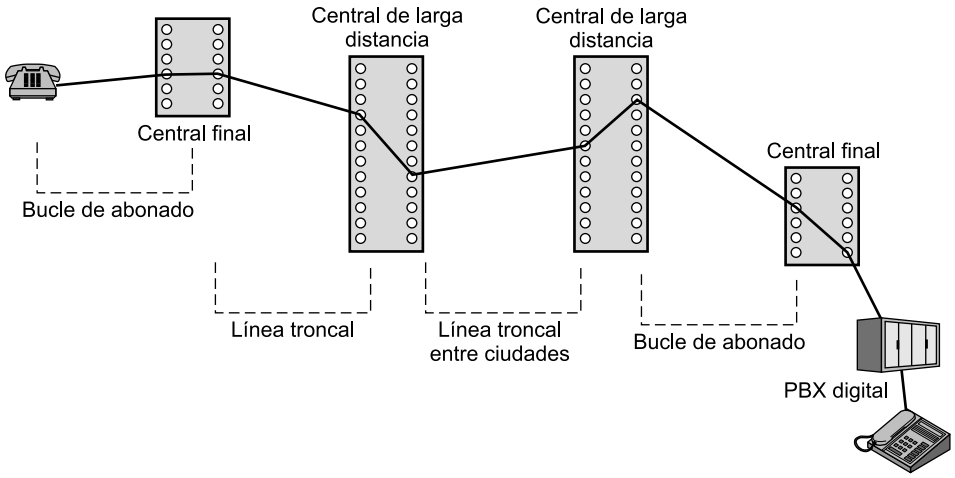


Figura 10.2. Ejemplo de conexión sobre una red pública de conmutación de circuitos.

ciones o sedes. Una red de este tipo consta normalmente de una serie de PBX, cada una de las cuales se sitúa en una sede y que están interconectadas entre sí a través de líneas alquiladas a alguno de los operadores de telecomunicaciones, como por ejemplo AT&T. Un último ejemplo de aplicación de la conmutación de circuitos es la conmutación de datos. Ésta es similar a las PBX, pero en este caso se interconectan dispositivos de procesamiento de datos digitales, como terminales y computadores.

Una red pública de telecomunicaciones se puede describir a través de los cuatro componentes que forman su arquitectura:

- **Abonados:** dispositivos que se conectan a la red. La mayoría de los dispositivos de abonado en redes de telecomunicación públicas continúan siendo en la actualidad los teléfonos, si bien el porcentaje de tráfico de datos crece año tras año.
- **Línea de abonado:** enlace entre el abonado y la red, también denominado *bucle de abonado* o *bucle local*. En casi todas las conexiones de bucle local se hace uso de cable de par trenzado. La longitud del bucle local está normalmente comprendida en el rango que va desde unos pocos kilómetros hasta varias decenas de ellos.
- **Centrales:** centros de conmutación de la red. Aquellos centros de conmutación a los que se conectan directamente los abonados se denominan *centrales finales*. Generalmente, una central final da servicio a varios miles de abonados en un área geográfica localizada. Existen alrededor de 19.000 centrales finales en los Estados Unidos, por lo que es claramente imposible en la práctica la existencia de un enlace directo entre cada dos centrales finales cualesquiera; esto requeriría del orden de 2×10^8 enlaces. En lugar de ello se utilizan nodos de conmutación intermedios.
- **Líneas troncales:** enlaces entre centrales. Las líneas troncales (*trunk*) transportan varios circuitos de voz haciendo uso de FDM o de TDM síncrona. Con anterioridad, al conjunto de estas líneas se le denominaba *sistema de transporte*.

Los abonados se conectan directamente a una central final, la cual conmuta el tráfico entre abonados y entre un abonado y otras centrales de larga distancia. Las otras centrales son responsables de encaminar y conmutar el tráfico entre centrales finales. Esta distinción se muestra en la Figura 10.3.

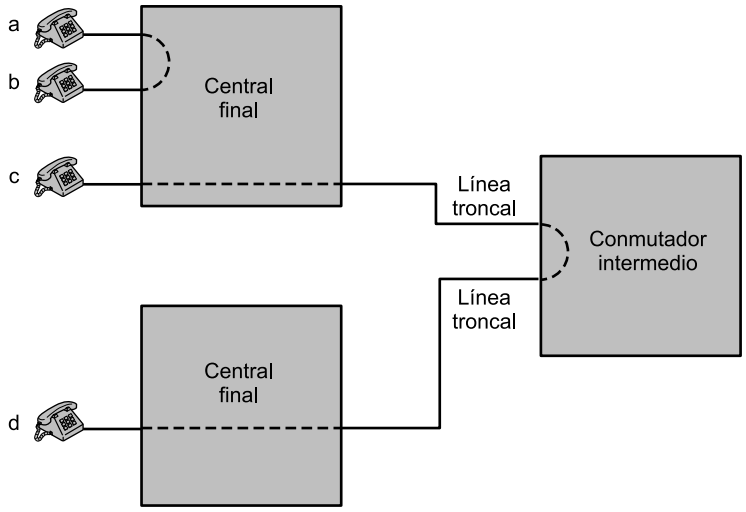


Figura 10.3. Establecimiento de un circuito.

Para comunicar entre sí dos abonados que están conectados a la misma central final, se establece un circuito entre ellos en la forma descrita anteriormente. Si los abonados están conectados a dos centrales finales diferentes, el circuito establecido entre ellos consistirá en una concatenación de circuitos a través de una o más centrales intermedias. En la citada figura se establece una conexión entre las líneas *a* y *b* simplemente mediante un circuito a través de la central final. Por su parte, la conexión entre *c* y *d* es más compleja. En este caso, la central final de *c* establece una conexión entre la línea *c* y un canal sobre una línea troncal TDM al conmutador intermedio. En este conmutador, el canal se conecta a un canal de un enlace TDM a la central final de *d*. En esta central final, el canal se conecta con la línea *d*.

La tecnología de conmutación de circuitos se desarrolló para las aplicaciones de tráfico de voz. Uno de los aspectos clave del tráfico de voz es que no debe haber prácticamente retardo en la transmisión ni, por supuesto, variaciones en el mismo. La velocidad de transmisión de la señal se debe mantener constante, ya que tanto la emisión como la recepción se realizan a la misma velocidad. Estos requisitos son necesarios para permitir una conversación humana normal. Es más, la calidad de la señal recibida debe ser suficientemente elevada para proporcionar, como mínimo, inteligibilidad.

La conmutación de circuitos está ampliamente extendida, ocupando una posición predominante debido a que es adecuada para la transmisión analógica de señales de voz. En el mundo digital actual resultan más relevantes sus limitaciones. No obstante, a pesar de sus inconvenientes, la conmutación de circuitos continúa siendo una atractiva alternativa tanto para redes de área local como para redes de área amplia. Una de sus ventajas principales es la transparencia: una vez que se ha establecido el circuito, éste parece una conexión directa entre las dos estaciones conectadas, no siendo necesaria la inclusión de lógica de red especial en las estaciones.

10.3. CONCEPTOS DE CONMUTACIÓN DE CIRCUITOS

Para comprender mejor la tecnología de conmutación de circuitos, consideremos un ejemplo del funcionamiento de un solo nodo conmutado. Una red diseñada en torno a un único nodo de conmutación de circuitos consiste en un conjunto de estaciones conectadas a una unidad central de con-

mutación. El conmutador central establecerá un canal dedicado entre dos dispositivos cualquiera que deseen comunicarse. En la Figura 10.4 se muestran los elementos principales de una red de un solo nodo como la mencionada. Las líneas discontinuas dentro del conmutador simbolizan las conexiones que se encuentran activas en un momento dado.

La parte central de todo sistema moderno es el **conmutador digital**, cuya función es proporcionar una ruta transparente entre dos dispositivos conectados cualquiera. El camino es transparente en el sentido de que parece como si existiese una conexión directa entre los dispositivos. Generalmente, la conexión debe permitir transmisión *full-duplex*.

El elemento de **interfaz de red** incluye las funciones y el hardware necesarios para conectar dispositivos digitales, como dispositivos de procesamiento de datos y teléfonos digitales, a la red. Los teléfonos analógicos también se pueden conectar si la interfaz de red contiene la lógica necesaria para convertir la señal a digital. Las líneas troncales a otros conmutadores digitales transportan señales TDM y proporcionan los canales para la construcción de redes de varios nodos.

La **unidad de control** realiza tres tareas generales. En primer lugar, establece conexiones, lo cual se realiza generalmente bajo demanda; es decir, ante la solicitud de un dispositivo conectado a la red. Para establecer la conexión, la unidad de control debe gestionar y confirmar la petición, determinar si la estación de destino está libre y construir una ruta a través del conmutador. En segundo lugar, la unidad de control debe mantener la conexión. Dado que el conmutador digital

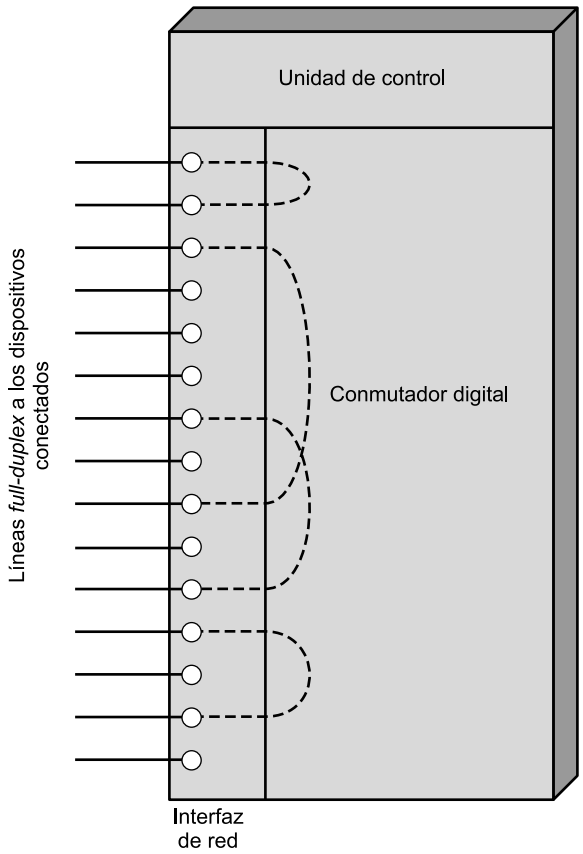


Figura 10.4. Elementos de un nodo de conmutación de circuitos.

utiliza una aproximación por división en el tiempo, esta segunda tarea puede precisar un control continuo de los elementos de conmutación. No obstante, los bits de la comunicación se transfieren de forma transparente (desde el punto de vista de los dispositivos del nodo). Por último, la unidad de control debe liberar la conexión, bien en respuesta a una solicitud generada por una de las partes o por razones propias.

Una característica importante de un dispositivo de conmutación de circuitos es si es *bloqueante* o *no bloqueante*. El bloqueo se produce cuando la red no puede conectar dos estaciones debido a que todos los posibles caminos entre ellas están siendo ya utilizados. Una red bloqueante es aquella en la que es posible el bloqueo. Por su parte, una red no bloqueante se caracteriza porque permite que todas las estaciones se conecten simultáneamente (por parejas) y garantiza el servicio a todas las solicitudes de conexión posibles siempre que el destino esté libre. La configuración bloqueante resulta generalmente aceptable cuando una red sólo admite tráfico de voz, ya que se espera que la mayor parte de las llamadas telefónicas sean de corta duración y que, por tanto, sólo una fracción de los teléfonos estén ocupados todo el tiempo. Sin embargo, estas suposiciones pueden no ser válidas cuando se trata de dispositivos de procesamiento de datos. Por ejemplo, para una aplicación de entrada de datos, un terminal puede estar continuamente conectado a un computador durante horas. Por tanto, para aplicaciones de datos se necesita una configuración no bloqueante o «casi no bloqueante» (es decir, con una probabilidad de bloqueo muy baja).

Veamos ahora las técnicas de conmutación internas a un nodo de conmutación de circuitos.

CONMUTACIÓN POR DIVISIÓN EN EL ESPACIO

La conmutación por división en el espacio se desarrolló originalmente para entornos analógicos, desplazándose posteriormente al contexto digital. Los principios fundamentales de un conmutador son los mismos tanto si se usa para transportar señales analógicas como para el transporte de señales digitales. Como su nombre indica, un conmutador por división en el espacio es aquel en el que las rutas de señal que se establecen son físicamente independientes entre sí (separadas en el espacio). Cada conexión necesita del establecimiento de un camino físico a través del conmutador que se dedique únicamente a la transferencia de señales entre los dos extremos. El bloque básico de un conmutador consiste en una matriz de conexiones metálicas (o puntos de cruce) o puertas semiconductoras que una unidad de control puede habilitar o deshabilitar.

En la Figura 10.5 se muestra una matriz de conexiones simple con 10 líneas de entrada/salida *full-duplex*. La matriz tiene 10 entradas y 10 salidas; cada estación se conecta a la matriz a través de una línea de entrada y otra de salida. La conexión entre dos líneas cualquiera es posible habilitando el punto de cruce correspondiente. Obsérvese que es necesario un total de 100 conexiones. Los conmutadores matriciales presentan varias limitaciones:

- El número de conexiones crece con el cuadrado del número de estaciones conectadas, lo cual resulta costoso para conmutadores grandes.
- La pérdida de un cruce impide la conexión entre los dos dispositivos cuyas líneas intersecccionan en ese punto de cruce.
- Las conexiones se utilizan de forma ineficiente; incluso cuando todos los dispositivos conectados se encuentran activos, sólo está ocupada una pequeña fracción de los puntos de cruce.

Para superar estas limitaciones se emplean conmutadores multietapa. La Figura 10.6 es un ejemplo de conmutador de tres etapas. Esta solución presenta dos ventajas respecto a una matriz de una sola etapa:

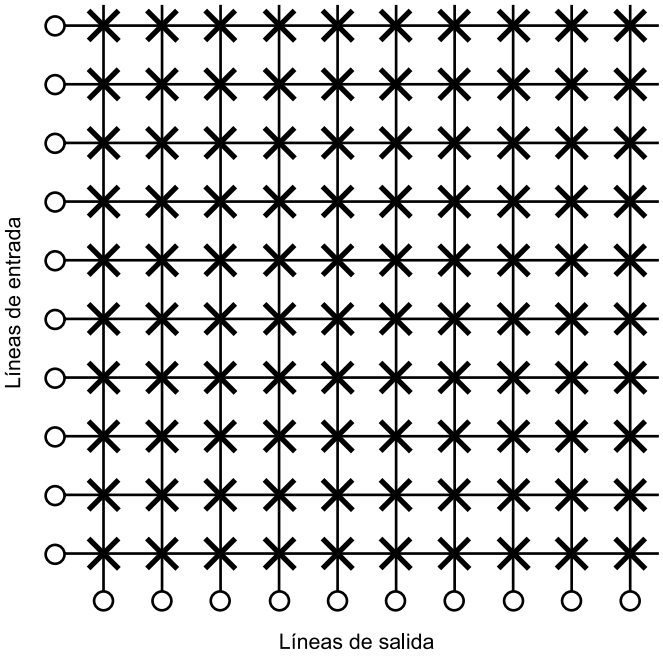


Figura 10.5. Conmutador por división en el espacio.

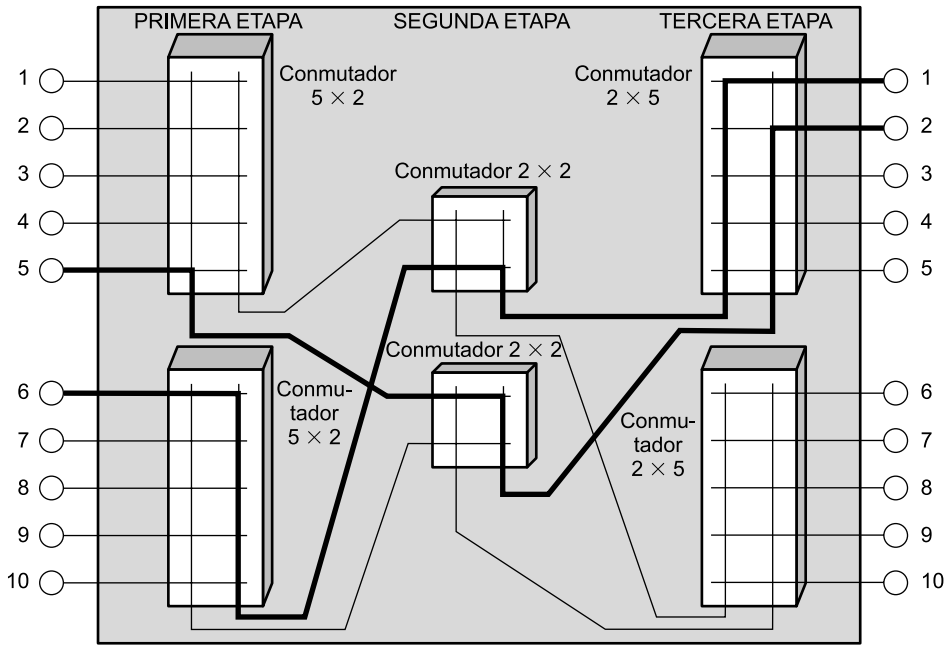


Figura 10.6. Conmutador por división en el espacio de tres etapas.

- El número de conexiones se reduce, aumentando la utilización de las líneas de cruce. En este ejemplo, el número total de interconexiones para 10 estaciones se reduce de 100 a 48.
- Existe más de una ruta a través de la red para conectar dos extremos, incrementándose así la fiabilidad de la misma.

Evidentemente, una red multietapa necesita un esquema de control más complejo. Para establecer un camino en una red de una etapa sólo se necesita habilitar una única puerta. En una red multietapa se debe determinar una ruta libre a través de las etapas, habilitando las puertas correspondientes.

Una cuestión importante acerca de un conmutador por división en el espacio multietapa es que puede ser bloqueante. Está claro a partir de la Figura 10.5 que una matriz de una sola etapa es no bloqueante; es decir, siempre hay un camino disponible para conectar una entrada con una salida. Como se muestra en la Figura 10.6, esto no es necesariamente cierto en el caso de un conmutador multietapa. En esta figura se resaltan en negrita las líneas ya en uso. En esta situación, la línea de entrada 10, por ejemplo, no se puede conectar a las líneas de salida 3, 4 o 5, aun cuando todas ellas estuviesen disponibles. Un conmutador multietapa puede convertirse en no bloqueante aumentando el número o el tamaño de los conmutadores intermedios, si bien ello incrementará el costo.

CONMUTACIÓN POR DIVISIÓN EN EL TIEMPO

La tecnología de conmutación tiene una larga historia, la mayor parte de la cual corresponde a la era analógica. Con la aparición de la voz digitalizada y las técnicas de multiplexación por división en el tiempo síncronas, se posibilita la transmisión de la voz y de los datos mediante señales digitales. Esto ha dado lugar a un cambio drástico en el diseño y en la tecnología de los sistemas de conmutación. En lugar de utilizar los sistemas relativamente torpes por división en el espacio, los sistemas digitales modernos se basan en el control inteligente de elementos de división en el espacio y de división en el tiempo.

Prácticamente todos los conmutadores de circuitos modernos emplean técnicas por división en el tiempo para el establecimiento y el mantenimiento de los circuitos. La conmutación por división en el tiempo involucra la fragmentación de una cadena de bits de menor velocidad en segmentos que compartirán una secuencia de velocidad superior con otras cadenas de bits. Los fragmentos individuales, o ranuras, se gestionan por parte de la lógica de control con el fin de encaminar los datos desde la entrada hacia la salida. Existen distintas variantes dentro de este concepto básico, si bien su estudio queda fuera de los objetivos de este libro.

10.4. SEÑALIZACIÓN DE CONTROL

En las redes de conmutación de circuitos, las señales de control constituyen el medio mediante el que se gestiona la red y por el que se establecen, mantienen y finalizan las llamadas. Tanto la gestión de las llamadas como la gestión de la red necesitan que se intercambie información entre el abonado y los conmutadores, entre los conmutadores entre sí y entre los conmutadores y el centro de gestión de red. En las grandes redes de telecomunicaciones se precisa un esquema de señalización de control relativamente complejo. En esta sección se ofrece un breve resumen de la funcionalidad de las señales de control, estudiándose posteriormente la técnica base de las redes digitales integradas modernas, denominada señalización por canal común.

FUNCIONES DE SEÑALIZACIÓN

Las señales de control afectan a varios aspectos relativos al funcionamiento de la red, incluyendo tanto los servicios de la red visibles por el abonado como los procedimientos internos. A medida que la red se hace más compleja, crece necesariamente el número de funciones que se realizan a través de la señalización de control. Entre las funciones más importantes se encuentran las siguientes:

1. Comunicación audible con el abonado, que incluye el tono de marcar, el tono de llamada, la señal de ocupado, etc.
2. Transmisión del número marcado a las centrales de conmutación, que tratarán de establecer una conexión.
3. Transmisión de información entre los conmutadores indicando que una llamada dada no se puede establecer.
4. Transmisión de información entre conmutadores indicando que una llamada ha finalizado y que la ruta puede desconectarse.
5. Generación de la señal que hace que el teléfono suene.
6. Transmisión de información con fines de tarifación.
7. Transmisión de información indicando el estado de los equipos y líneas principales de la red. Esta información se puede emplear con fines de encaminamiento y mantenimiento.
8. Transmisión de información utilizada para el diagnóstico y aislamiento de fallos en el sistema.
9. Control de equipos especiales como equipos para canales vía satélite.

Como ejemplo del empleo de la señalización de control, considérese la secuencia de conexión telefónica típica desde una línea a otra en la misma central:

1. Ambos teléfonos deben estar libres (colgados) antes de la llamada. Ésta empieza cuando uno de los abonados toma el auricular (descuelga), lo cual se indica automáticamente al conmutador de la central final a la que está conectado.
2. El conmutador responde con un tono audible de marcar, señalizando al abonado que puede marcar el número deseado.
3. El abonado llamante marca el número, lo cual se comunica al conmutador como la dirección del abonado de destino.
4. Si el abonado llamado no está ocupado, el conmutador lo alerta acerca de la llamada entrante enviando una señal de llamada que provoca que su teléfono suene.
5. El conmutador proporciona realimentación al abonado llamante:
   - **a)** Si el abonado destino no está ocupado, el conmutador devuelve un tono audible de llamada al abonado origen mientras que, simultáneamente, se envía la señal de llamada al abonado llamado.
   - **b)** Si el destino está ocupado, el conmutador envía una señal audible de ocupado al llamante.
   - **c)** Si la llamada no puede establecerse a través del conmutador, éste envía un mensaje audible de «reintento» al abonado llamante.

6. El destino acepta la llamada levantando el auricular (descolgando), lo que se comunica automáticamente al conmutador.

7. El conmutador corta la señal y el tono de llamada, estableciendo una conexión entre los dos abonados.

8. La conexión se libera cuando una de las dos partes cuelga.

Cuando el abonado llamado se encuentra conectado a un conmutador diferente al que lo está el abonado origen, son necesarias las siguientes funciones de señalización en los enlaces que unen los conmutadores:

1. El conmutador origen ocupa un enlace libre entre ambos conmutadores, envía una indicación de descolgar a través del enlace y solicita un registro de dígitos al otro conmutador para comunicar la dirección destino.

2. El conmutador final envía una señal de descolgar seguida por una de colgar, conocida como «parpadeo» o «guiño». Esto indica que el registro está preparado.

3. El conmutador origen envía los dígitos de la dirección al conmutador final.

Este ejemplo ilustra algunas de las funciones realizadas por las señales de control. Las funciones realizadas por las señales de control se pueden agrupar básicamente en cuatro clases: de supervisión, de direccionamiento, de información sobre la llamada y de gestión de la red.

El término **supervisión** se emplea generalmente para referirnos a las funciones de control que tienen un carácter binario (verdadero/falso; activado/desactivado), como solicitud de servicio, respuesta, aviso y retorno a desocupado. Estas señales se encargan de informar acerca de la disponibilidad del abonado llamado y de los recursos de la red necesarios. Las señales de control de supervisión se usan para determinar si un recurso necesario está disponible y, si es así, reservarlo. También se utilizan para comunicar el estado de los recursos que se han solicitado.

Las señales de **direccionamiento** identifican al abonado. Inicialmente se genera una señal de dirección por parte de un abonado origen cuando marca un número de teléfono. La dirección resultante se puede propagar a través de la red para permitir el encaminamiento, así como localizar y hacer que suene el teléfono del abonado destino.

El término **información sobre la llamada** se refiere a aquellas señales que proporcionan al abonado información acerca del estado de la llamada. Éstas contrastan con las señales de control internas entre conmutadores utilizadas en el establecimiento y cierre de la llamada. Las señales internas a la red son mensajes eléctricos analógicos o digitales; en cambio, las señales de información sobre la llamada son tonos audibles que pueden ser oídos por el llamante o por un operador que disponga del equipo de teléfono apropiado.

Las señales de supervisión, de direccionamiento y de control de información sobre la llamada están directamente involucradas en el establecimiento y finalización de una llamada. Por el contrario, las señales de **gestión de la red** se utilizan para el mantenimiento, la resolución de problemas y el funcionamiento general de la red. Estas señales pueden tener forma de mensajes, como por ejemplo una lista de rutas predefinidas enviadas a una estación para la actualización de sus tablas de encaminamiento. Las señales de gestión de la red cubren un amplio abanico de funciones, y será esta clase de señales la que más se extenderá con la creciente complejidad de las redes conmutadas.

LOCALIZACIÓN DE LA SEÑALIZACIÓN

Es necesario considerar la señalización de control en dos contextos: la señalización entre el abonado y la red y la señalización dentro de la red. Generalmente, la señalización funciona de forma diferente en dichos contextos.

La señalización entre un teléfono, o cualquier otro dispositivo de abonado, y la oficina de conmutación a la que se encuentra conectado se determina, en gran medida, por las características del dispositivo del abonado y por las necesidades del usuario. Las señales dentro de la red corresponden completamente a intercambios entre computadores. Esta señalización interna no se ocupa sólo de la gestión de llamadas del abonado, sino también de la gestión de la propia red. Así, para la señalización interna se necesita un conjunto más complejo de órdenes, respuestas y parámetros.

Dado que se utilizan dos técnicas de señalización diferentes, la central local de conmutación a la que está conectado el abonado debe proporcionar una correspondencia o traducción entre la técnica de señalización relativamente poco compleja usada por el abonado y la técnica de mayor complejidad utilizada internamente en la red.

SEÑALIZACIÓN POR CANAL COMÚN

La señalización de control tradicional en redes de conmutación de circuitos se ha realizado a través de la propia línea troncal o intracanal. En la técnica de **señalización intracanal** se usa el mismo canal para transportar tanto las señales de control como la propia llamada. Esta señalización comienza en el abonado origen y sigue la misma ruta que la llamada en sí. Esto tiene la ventaja de que no se precisan servicios de transmisión adicionales para llevar a cabo la señalización; los recursos para transmisión de voz son compartidos por la señalización de control.

Existen dos formas de señalización intracanal: intrabanda y fuera de banda. La **señalización intrabanda**, o en banda, utiliza no sólo el mismo camino físico que la llamada a la que sirve, sino que usa también la misma banda de frecuencias que las señales de voz transmitidas. Esta técnica de señalización presenta varias ventajas. Dado que las señales de control tienen las mismas propiedades electromagnéticas que las señales de voz, pueden llegar a los mismos lugares que éstas. Por tanto, no existe limitación alguna para el uso de la señalización intrabanda en cualquier punto de la red, incluso en aquellos sitios donde tiene lugar la conversión analógica a digital o digital a analógica. Además, es imposible establecer una llamada sobre un canal de voz con errores, ya que las señales de control usadas en el establecimiento de la ruta tendrían que seguir el mismo camino.

La **señalización fuera de banda** aprovecha el hecho de que las señales de voz no utilizan completamente los 4 kHz de ancho de banda reservado para ellas, de modo que dentro de los 4 kHz se hace uso de una banda de señalización estrecha e independiente para el envío de las señales de control. La principal ventaja de esta aproximación radica en que las señales de control se pueden enviar tanto si hay como si no señales de voz en la línea, permitiéndose así la supervisión y el control continuos de la llamada. No obstante, en un esquema fuera de banda se necesita circuitería electrónica adicional para gestionar la banda de señalización; además, las velocidades de señalización son inferiores, ya que la señal se ha confinado en un ancho de banda estrecho.

A medida que las redes de telecomunicaciones públicas se han hecho más complejas y ofrecen un conjunto de servicios más amplio, se hacen más evidentes las desventajas que presenta la señalización intracanal. En primer lugar, la velocidad de transferencia de información se encuentra bastante limitada. Con las señales en banda, un canal de voz en uso sólo puede ser utilizado por las señales de control cuando no hay señales de voz en el circuito. En la señalización fuera de banda

se encuentra disponible un ancho de banda muy estrecho. Con estas limitaciones resulta difícil transmitir a tiempo el más simple de los mensajes de control; en cambio, se precisa un repertorio de señales de control más amplio y potente con el fin de aprovechar los servicios potenciales y hacer frente a la creciente complejidad de las nuevas tecnologías de red.

Una segunda desventaja de la señalización intracanal es el retardo existente desde que un abonado introduce una dirección (marca el número) hasta que la conexión se establece. La necesidad de reducir este retardo es cada vez más importante en la medida en que las redes se están utilizando para nuevas aplicaciones. Por ejemplo, en las llamadas controladas por computador, como el procesamiento de transacciones, se transmiten mensajes relativamente cortos, por lo que el tiempo de establecimiento de llamada representa una parte importante del tiempo de transacción total.

Ambos problemas se pueden evitar mediante la **señalización por canal común**, en la que las señales de control se transmiten por rutas completamente independientes de los canales de voz (*véase* Tabla 10.1). Una ruta independiente para las señales de control puede transportar las señales de varios canales de abonado, siendo, en consecuencia, un canal de control común para todos estos canales de abonado.

Tabla 10.1. Técnicas de señalización en redes de conmutación de circuitos.

	Descripción	Comentario
Intracanal		
Intrabanda	Se transmiten las señales de control en la misma banda de frecuencias usada por las señales de voz.	Es la técnica más sencilla. Es necesaria para las señales de información sobre la llamada y se puede usar para otras señales de control. La señalización intrabanda se puede utilizar sobre cualquier tipo de interfaz de línea de abonado.
Fuera de banda	Las señales de control se transmiten haciendo uso de los mismos recursos que las señales de voz, pero en una parte diferente de la banda de frecuencias.	A diferencia de la señalización intrabanda, la señalización fuera de banda proporciona una supervisión continua durante toda la conexión.
Por canal común	Las señales de control se transmiten sobre canales de señalización dedicados a las señales de control y son comunes a varios canales de voz.	Se reduce el tiempo de establecimiento de llamada en comparación con los métodos de señalización intracanal. Resulta también más adaptable a las nuevas necesidades funcionales.

El fundamento de la señalización por canal común se ilustra y compara con la señalización intracanal en la Figura 10.7. Como se puede observar, la ruta de señal para la señalización por canal común está físicamente separada de la ruta de voz u otras señales de abonado. El canal común se puede configurar con el ancho de banda necesario para transportar señales de control que lleven a cabo una gran variedad de funciones. Así, tanto el protocolo de señalización como la arquitectura de red que lo soporta son más complejos que en la señalización intracanal. Sin embargo, la reducción continua en los costes del hardware de los computadores hace que la señalización por canal común resulte cada vez más atractiva. Las señales de control son mensajes que se transfieren entre los conmutadores y entre el conmutador y el centro de gestión de red. De este modo, la parte de señalización de control de la red es, en efecto, una red distribuida de computadores que transporta mensajes cortos.

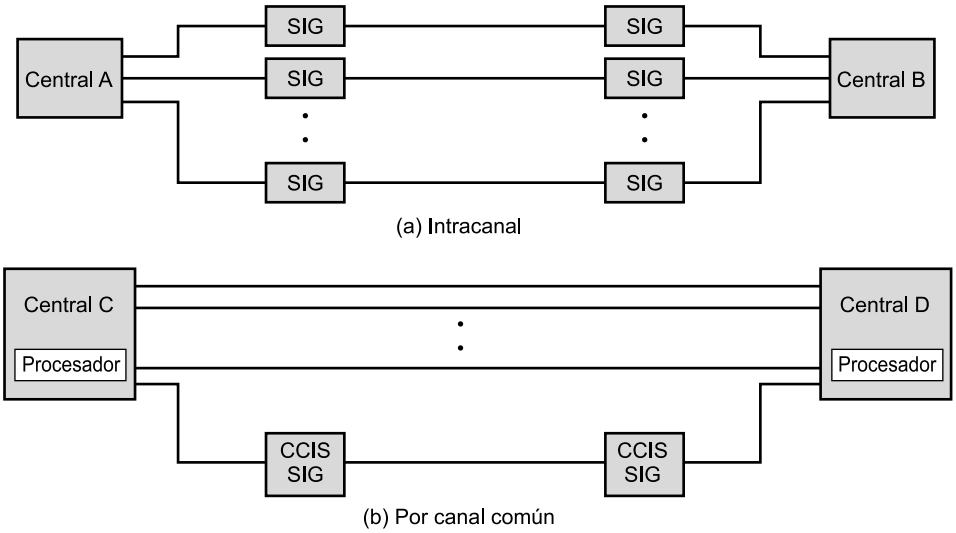


Figura 10.7. Señalización intracanal y por canal común.

Existen dos modos de funcionamiento en la señalización por canal común (*véase* Figura 10.8). En el **modo asociado**, el canal común sigue los pasos, a lo largo de toda la línea, a los grupos troncales entre conmutadores a los que sirve entre los dos extremos. Las señales de control viajan en canales diferentes a los de las señales de abonado y, dentro de un mismo conmutador, las señales de control se encaminan directamente hacia un procesador de señales de control. Un modo más complejo, aunque más potente, es el **modo no asociado**. En este modo se hace crecer la red a través de la adición de nodos llamados puntos de transferencia de señal. En este caso no existe una asignación o correspondencia ni definitiva ni sencilla entre los canales de control y los grupos troncales. En efecto, en este modo existen ahora dos redes separadas, con enlaces entre ellas de modo que la parte de control de la red puede realizar sus funciones a través de los nodos de conmutación que están dando servicio a las llamadas de abonado. La gestión de la red resulta más fácil en el modo no asociado ya que los canales de control se pueden asignar a tareas de una manera más flexible. El modo no asociado es el usado en RDSI.

Con la señalización intracanal, las señales de control de un conmutador dado se generan en un procesador de control y posteriormente se conmutan sobre el canal de salida correspondiente. En el receptor, las señales de control se deben conmutar desde el canal de voz al procesador de control. En la señalización por canal común, las señales de control se transfieren directamente desde un procesador al siguiente, sin ser asociadas a un canal de voz. Este procedimiento es más sencillo y menos susceptible a interferencias, tanto accidentales como intencionadas, entre la señal del abonado y las de control. Ésta es una de las razones principales que justifican el empleo de la señalización por canal común. Otra razón importante para ello es la reducción conseguida en el tiempo de establecimiento de llamada. Considérese la secuencia de eventos para el establecimiento de llamada en la señalización intracanal cuando está implicado más de un conmutador. Se enviará una señal de control desde un conmutador hasta el siguiente a través de la ruta correspondiente. En cada conmutador, la señal no se transferirá hacia el siguiente enlace de la ruta hasta que no se haya establecido el circuito asociado a través de dicho conmutador. La retransmisión de información de control en la técnica de señalización por canal común se puede solapar con el procedimiento de establecimiento del circuito.

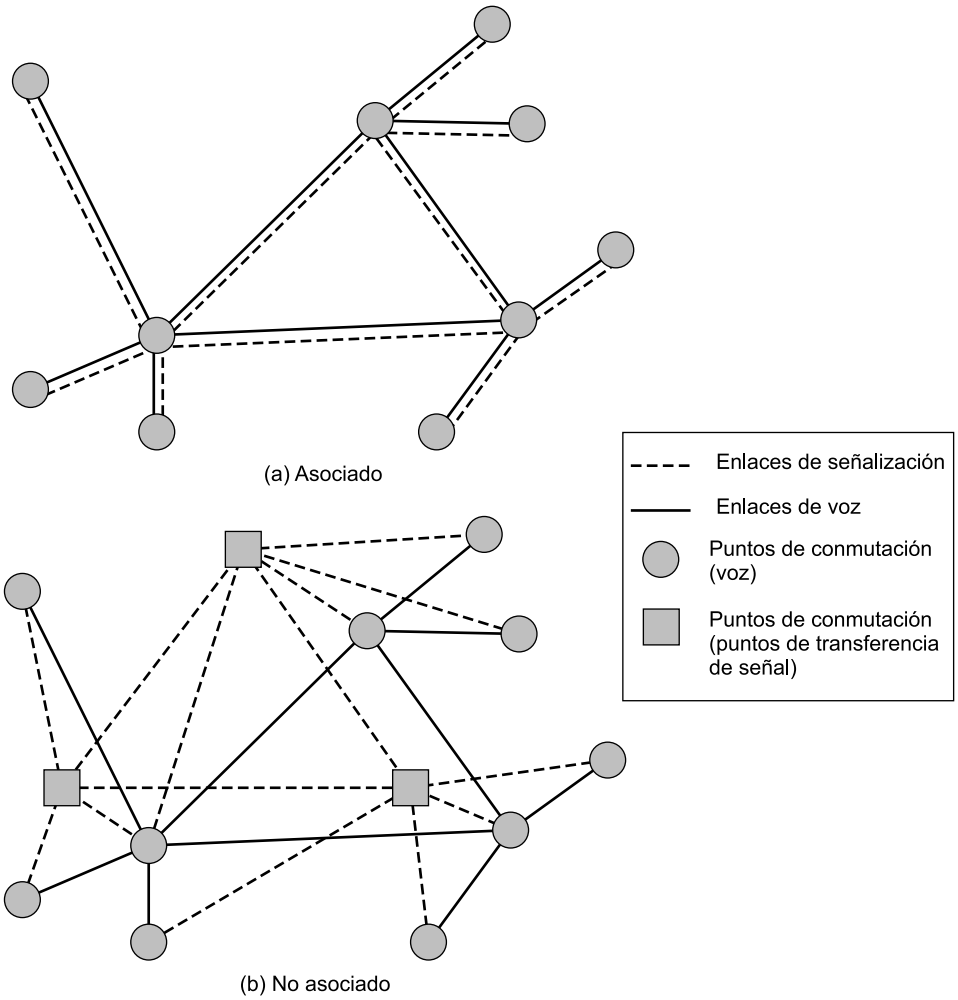


Figura 10.8. Modos de señalización por canal común [FREE96].

La señalización no asociada presenta una ventaja adicional: se pueden establecer uno o más puntos centrales de control. Toda la información de control se puede encaminar a un centro de control de red, en el que se procesan las solicitudes y desde el que se envían las señales de control a los conmutadores que gestionan el tráfico de los abonados. De esta forma, las solicitudes se pueden procesar teniendo en cuenta una visión más global del estado de la red.

Por supuesto, la señalización por canal común tiene algunas desventajas. Éstas están relacionadas en primer lugar con la complejidad de la técnica; sin embargo, la reducción de costes en el hardware digital y el creciente carácter digital de las redes de telecomunicaciones hacen que la señalización por canal común sea la tecnología apropiada en la actualidad.

Todo el estudio presentado a lo largo de esta sección se ha centrado en el uso de la señalización por canal común dentro de la red (es decir, para controlar los conmutadores). Incluso en el caso de que la red esté completamente controlada mediante señalización por canal común, será necesaria alguna señalización en banda para la comunicación con el abonado. Por ejemplo, el tono de marcar, la señal de indicación de llamada y la señal de ocupación deben ser señales intracanal

dirigidas hacia el usuario. En una red telefónica sencilla, el abonado no tendrá acceso a la parte de la red señalizada por canal común, por lo que no tendrá que utilizar el protocolo correspondiente. Sin embargo, en redes digitales más sofisticadas, incluida la RDSI, se utiliza un protocolo de señalización por canal común entre el abonado y la red, que se hace corresponder con el protocolo de señalización interno.

SISTEMA DE SEÑALIZACIÓN NÚMERO 7

La señalización por canal común es más flexible y potente que la señalización intracanal, y está mejor preparada para satisfacer las necesidades de las redes digitales integradas. El esquema más ampliamente usado en este contexto es el sistema de señalización número 7 (SS7, *Signaling System Number* 7). Si bien SS7 ha sido específicamente diseñado para su uso en redes RDSI, se ideó con ánimo de ser una norma de señalización por canal común abierta que se pudiera utilizar en diversas redes de conmutación de circuitos digitales. SS7 es el mecanismo que proporciona el control interno y la inteligencia de red esenciales a una red RDSI.

El objetivo de SS7 es proporcionar un sistema de señalización por canal común de propósito general estandarizado internacionalmente con las siguientes características principales:

- Optimizado para su utilización en redes digitales de telecomunicaciones con nodos digitales controlados por programa y que hacen uso de canales digitales a 64 kbps.
- Diseñado para satisfacer las necesidades, tanto actuales como futuras, de transferencia de información para control de llamadas, control remoto, gestión y mantenimiento.
- Diseñado con objeto de constituir un medio fiable para la transferencia de información en el orden correcto sin pérdidas ni duplicaciones.
- Apropiado para su uso en canales analógicos y a velocidades inferiores a 64 kbps.
- Adecuado para enlaces terrestres y satélite punto a punto.

El ámbito de acción del protocolo SS7 es enorme, dado que cubre todos los aspectos de la señalización de control en redes digitales complejas, incluyendo el encaminamiento fiable y el envío de mensajes de control y del contenido orientado a aplicación de los mismos. En esta sección se ofrece un breve estudio del protocolo SS7.

En SS7, los mensajes de control se encaminan a través de la red para llevar a cabo la gestión de las llamadas (establecimiento, mantenimiento, terminación) y las funciones relativas a la gestión de la red. Estos mensajes son bloques o paquetes pequeños que se pueden encaminar a través de la red, de modo que, aunque la red que está siendo controlada sea una red de conmutación de circuitos, la señalización de control se basa en la tecnología de conmutación de paquetes. De hecho, la red de conmutación de circuitos se recubre por una de conmutación de paquetes para llevar a cabo el control y funcionamiento de la primera.

SS7 define las funciones realizadas en la red de conmutación de paquetes, pero no especifica ninguna implementación hardware concreta. Por ejemplo, todas las funciones de SS7 se pueden implementar en los nodos de conmutación de circuitos como funciones adicionales de los mismos; esta aproximación corresponde al modo de señalización asociado mostrado en la Figura 10.8a. Como alternativa, en la Figura 10.8b se muestra el uso de puntos de conmutación independientes para el transporte exclusivo de los paquetes de control. Incluso en este caso, los nodos de conmutación de circuitos necesitarían implementar partes del protocolo SS7 con el fin de poder recibir señales de control.

Elementos de la red de señalización

SS7 define tres entidades funcionales: puntos de señalización, puntos de transferencia de señal y enlaces de señalización. Un **punto de señalización** (SP, *Signaling Point*) es un nodo de la red de señalización con capacidad de gestión de mensajes de control SS7. Un SP puede ser un receptor de mensajes de control incapaz de procesar mensajes que no vayan destinados directamente a él. Los nodos de conmutación de circuitos de la red podrían ser, por ejemplo, los extremos origen o destino de una comunicación. Otro ejemplo de SP lo constituye un centro de control de red. Un **punto de transferencia de señal** (STP, *Signal Transfer Point*) es un punto de señalización capaz de encaminar mensajes de control; es decir, un mensaje recibido sobre un enlace de señalización se transfiere a otro enlace. Un STP podría consistir en un nodo de encaminamiento puro, pudiendo realizar también las funciones propias de un punto final (origen/destino) de comunicaciones. Finalmente, un **enlace de señalización** es un enlace de datos que conecta entre sí puntos de señalización.

En la Figura 10.9 se evidencia la distinción entre la función de señalización mediante conmutación de paquetes y la función de transferencia de información basada en conmutación de circuitos para el caso de una arquitectura de señalización no asociada. Se puede considerar la existencia de dos planos de operación. El **plano de control** es responsable del establecimiento y de la gestión de las conexiones, las cuales se solicitan por parte del usuario. El diálogo entre éste y la red se realiza entre el usuario y el conmutador local. Con este fin, el conmutador local funciona como un punto de señalización, ya que debe llevar a cabo la conversión entre el diálogo con el usuario y los mensajes de control internos a la red, que son los que realmente realizan las acciones (SS7) solicitadas por el usuario. El protocolo SS7 se usa internamente a la red para establecer y mantener una conexión dada; este proceso puede involucrar a uno o más puntos de señalización y de transferencia de señal. Una vez que se ha establecido la conexión, la información se transfiere desde un usuario hasta el otro, extremo a extremo, en el **plano de información**. Para ello se establece un circuito desde el conmutador local de un usuario hasta el del otro, habiéndose realizado quizá el encaminado a través de uno o más nodos de conmutación de circuitos, denominados *centros de tránsito*. Todos estos nodos (conmutadores locales, centros de tránsito) son también puntos de señalización, ya que son capaces de enviar y recibir mensajes SS7 para establecer y gestionar la conexión.

Estructuras de la red de señalización

Las redes complejas disponen generalmente tanto de puntos de señalización (SP) como de puntos de transferencia de señal (STP). Una red de señalización que incluye nodos SP y nodos STP puede considerarse que tiene una estructura jerárquica en la que los SP constituyen el nivel inferior y los STP representan el nivel superior. Estos últimos pueden dividirse, a su vez, en varios niveles STP. En la Figura 10.9 se muestra un ejemplo correspondiente a una red con un solo nivel de STP.

Varios son los parámetros que pueden influir en las decisiones relativas al diseño de la red y al número de niveles a considerar:

- **Capacidad de los STP:** incluye el número de enlaces de señalización que puede gestionar un STP, el tiempo de transferencia de los mensajes de señalización y la capacidad en términos de mensajes.
- **Prestaciones de la red:** comprende el número de SP y los retardos de señalización.
- **Disponibilidad y fiabilidad:** mide la capacidad de la red para proveer servicios ante la ocurrencia de fallos en los STP.

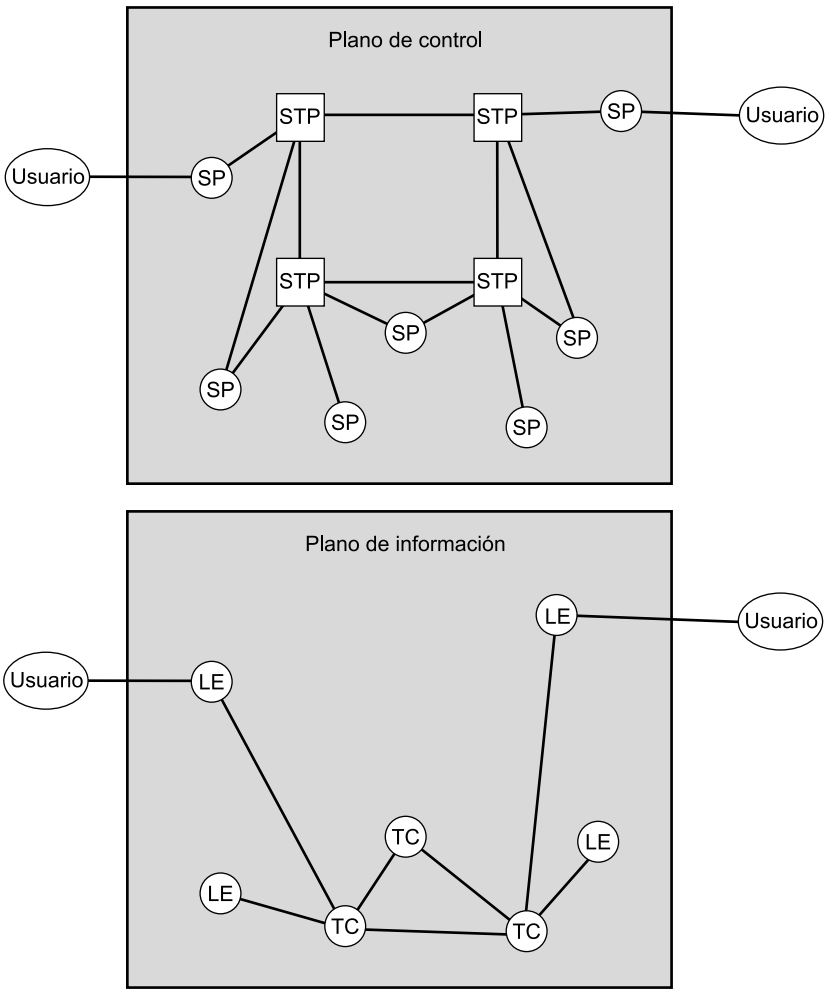


Figura 10.9. Puntos de señalización y de transferencia de información en SS7.

Cuando se consideran las restricciones de la red desde el punto de vista de las prestaciones, parece más adecuada la consideración de un solo nivel STP. Sin embargo, la consideración de los parámetros de disponibilidad y fiabilidad puede requerir un diseño con más de un nivel. La ITU-T sugiere las siguientes pautas:

- En una red de señalización jerárquica con un único nivel de STP:
  - — Cada SP que no sea simultáneamente un STP se conecta con, al menos, dos STP.
  - — El entramado de STP debe ser tan completo como sea posible, entendiendo por entramado completo aquel en el que existe un enlace directo entre dos STP cualquiera.
- En una red de señalización jerárquica con dos niveles de STP:
  - — Cada SP que no sea al mismo tiempo un STP se conecta con, al menos, dos STP del nivel inferior.

— Cada STP del nivel inferior se conecta con, al menos, dos STP del nivel superior.

— Los STP del nivel superior forman un entramado completo.

El diseño jerárquico en dos niveles de STP es generalmente tal que el nivel inferior se dedica a la gestión del tráfico correspondiente a una región geográfica particular de la red, mientras que el nivel superior gestiona el tráfico entre regiones.

10.5. ARQUITECTURA DE CONMUTACIÓN LÓGICA

La última tendencia en la tecnología de conmutación de circuitos se denomina usualmente *conmutación lógica* (*softswitch* en inglés). Esencialmente, un conmutador lógico es un computador de propósito general que ejecuta un software especializado que lo convierte en un conmutador telefónico inteligente. El coste de un *softswitch* es significativamente inferior al de un conmutador de circuitos tradicional, al tiempo que proporciona una mayor funcionalidad. En particular, adicionalmente a las funciones de conmutación de circuitos tradicionales, un *softswitch* puede convertir una secuencia de bits de voz digitalizada en paquetes. Esto abre las puertas a numerosas opciones relativas a la transmisión, entre las que se encuentra la cada vez más popular voz sobre IP (*Internet Protocol*).

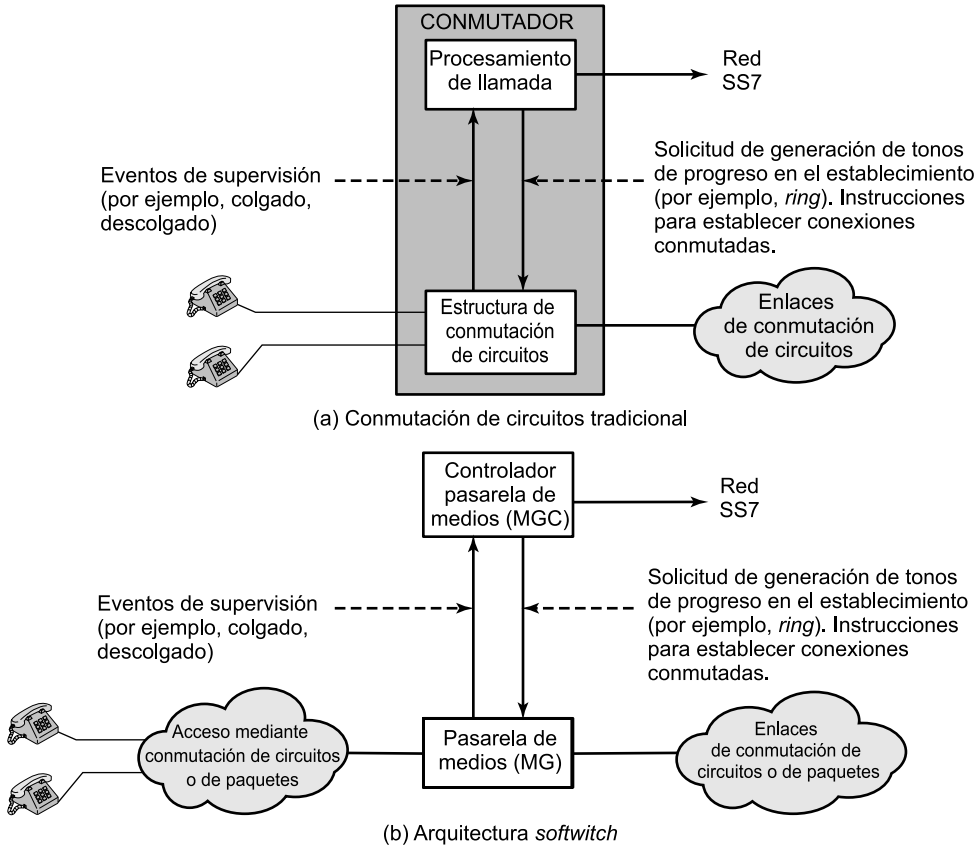

CONMUTADOR
Procesamiento de llamada
Red SS7
Eventos de supervisión (por ejemplo, colgado, descolgado)
Solicitud de generación de tonos de progreso en el establecimiento (por ejemplo, ring). Instrucciones para establecer conexiones conmutadas.
Estructura de conmutación de circuitos
Enlaces de conmutación de circuitos
(a) Conmutación de circuitos tradicional
Controlador pasarela de medios (MGC)
Red SS7
Eventos de supervisión (por ejemplo, colgado, descolgado)
Solicitud de generación de tonos de progreso en el establecimiento (por ejemplo, ring). Instrucciones para establecer conexiones conmutadas.
Acceso mediante conmutación de circuitos o de paquetes
Pasarela de medios (MG)
Enlaces de conmutación de circuitos o de paquetes
(b) Arquitectura softwitch

Figura 10.10. Comparación entre la conmutación de circuitos tradicional y la conmutación lógica (*softswitch*).

El elemento más complejo existente en un conmutador telefónico es el software que controla el procesamiento de las llamadas. Este software lleva a cabo el encaminamiento de las llamadas e implementa la lógica de procesamiento de llamada necesaria para la gestión de cientos de características del usuario llamante. Generalmente, este software se ejecuta en un procesador propietario integrado físicamente en el hardware de conmutación de circuitos. Una alternativa más flexible consiste en separar físicamente la función de procesamiento de llamada de la función de conmutación hardware. En terminología *softswitch*, la función de conmutación física la realiza una **pasarela de medios** (MG, *Media Gateway*), mientras que la lógica de procesamiento de llamada reside en un **controlador pasarela de medios** (MGC, *Media Gateway Controller*).

En la Figura 10.10 se compara la arquitectura de un conmutador de circuitos telefónico tradicional con la de un conmutador lógico o *softswitch*. En el último, el MG y el MGC son entidades diferentes y pueden ser adquiridas de proveedores distintos. Para facilitar la interoperatividad, se ha definido un protocolo de control de pasarela de medios entre el MG y el MGC (RFC 3015).

10.6. PRINCIPIOS DE CONMUTACIÓN DE PAQUETES

Las redes de telecomunicaciones de conmutación de circuitos de larga distancia se diseñaron originalmente para el tráfico de voz, siendo aún hoy en día la voz la responsable de la mayor parte del tráfico en estas redes. Una característica fundamental de las redes de conmutación de circuitos es que se dedican recursos internos de la red a una llamada particular; de este modo, para conexiones de voz, el circuito resultante alcanza un alto porcentaje de utilización, puesto que la mayor parte del tiempo está hablando un extremo o el otro. Sin embargo, a medida que las redes de conmutación de circuitos se han ido utilizando de forma creciente para conexiones de datos, se han puesto de manifiesto dos problemas:

- En una conexión de datos usuario/estación típica (por ejemplo, un usuario de un computador personal conectado a un servidor de base de datos) la línea está desocupada la mayor parte del tiempo. Por tanto, la técnica de conmutación de circuitos resulta ineficiente para conexiones de datos.
- En una red de conmutación de circuitos, la conexión ofrece una velocidad de datos constante, de modo que los dos dispositivos conectados deben transmitir y recibir a la misma velocidad. Esto limita la utilidad de la red para la interconexión de distintos tipos de computadores y estaciones de trabajo.

Para comprender cómo aborda estos problemas la conmutación de paquetes, veamos de forma breve el funcionamiento de esta técnica de conmutación. Los datos se transmiten en paquetes cortos, siendo 1.000 octetos un límite superior típico de la longitud de los mismos. Si un emisor tiene que enviar un mensaje de mayor longitud, éste se segmenta en una serie de paquetes (*véase* Figura 10.11). Cada paquete contiene una parte (o todas en el caso de que se trate de un mensaje corto) de los datos de usuario más cierta información de control. Esta información comprende, como mínimo, la que necesita la red para encaminar el paquete a través de ella y alcanzar el destino deseado. En cada nodo de la ruta, el paquete se recibe, se almacena temporalmente y se envía al siguiente nodo.

Volvamos a la Figura 10.1, pero consideremos ahora que la red que en ella se muestra es una red de conmutación de paquetes. Supóngase que se envía un paquete desde la estación A a la estación E. El paquete incluirá información de control indicando que el destino es E. El paquete se envía desde A al nodo 4, el cual almacena el paquete, determina el siguiente nodo en la ruta (digamos 5) y pone en cola el paquete en ese enlace (línea 4-5). Cuando el enlace está disponible, el

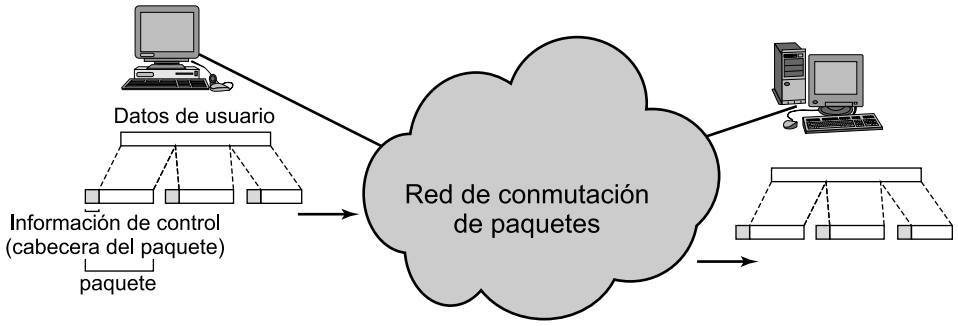


Figura 10.11. Utilización de paquetes.

paquete se transmite hacia el nodo 5, quien lo enviará hacia 6, y éste, finalmente, hacia E. Esta aproximación presenta varias ventajas frente a la conmutación de circuitos:

- La eficiencia de la línea es superior, ya que un único enlace entre dos nodos se puede compartir dinámicamente en el tiempo entre varios paquetes. Los paquetes forman una cola y se transmiten sobre el enlace tan rápidamente como es posible. Por el contrario, en la conmutación de circuitos, la capacidad temporal de un enlace se reserva a priori mediante la utilización de la técnica de multiplexación por división en el tiempo síncrona. Dicho enlace puede estar desocupado la mayor parte del tiempo, puesto que una parte de éste se dedica a una conexión sin datos.
- Una red de conmutación de paquetes puede realizar una conversión en la velocidad de los datos. Dos estaciones de diferente velocidad pueden intercambiar paquetes, ya que cada una se conecta a su nodo con una velocidad particular.
- Cuando aumenta el tráfico en una red de conmutación de circuitos algunas llamadas se bloquean; es decir, la red rechaza la aceptación de solicitudes de conexión adicionales mientras no disminuya la carga de la red. En cambio, en una red de conmutación de paquetes éstos siguen aceptándose, si bien aumenta el retardo en la transmisión.
- Se puede hacer uso de prioridades, de modo que si un nodo tiene varios paquetes en cola para su transmisión, éste puede transmitir primero aquellos con mayor prioridad. Estos paquetes experimentarán así un retardo menor que los de prioridad inferior.

TÉCNICA DE CONMUTACIÓN

Si una estación tiene que enviar un mensaje de longitud superior a la del tamaño máximo del paquete permitido a través de una red de conmutación de paquetes, fragmenta el mensaje en paquetes y los envía, de uno en uno, hacia la red. La cuestión que surge es cómo gestiona la red esta secuencia de paquetes para encaminarlos en su seno y entregarlos en el destino deseado. Existen dos aproximaciones usadas en las redes actuales: datagramas y circuitos virtuales.

En la técnica de **datagramas** cada paquete se trata de forma independiente, sin referencia alguna a los paquetes anteriores. Esta técnica se muestra en la Figura 10.12. Cada nodo elige el siguiente nodo en la ruta del paquete de acuerdo con información recibida de los nodos vecinos acerca de tráfico, fallo en las líneas, etc. De este modo, no todos los paquetes, aunque con el mismo destino, seguirán la misma ruta —*véase* subfigura (c)—, pudiendo recibirse desordenados en el último nodo. En este ejemplo, el nodo final almacena todos los paquetes y los reordena antes de

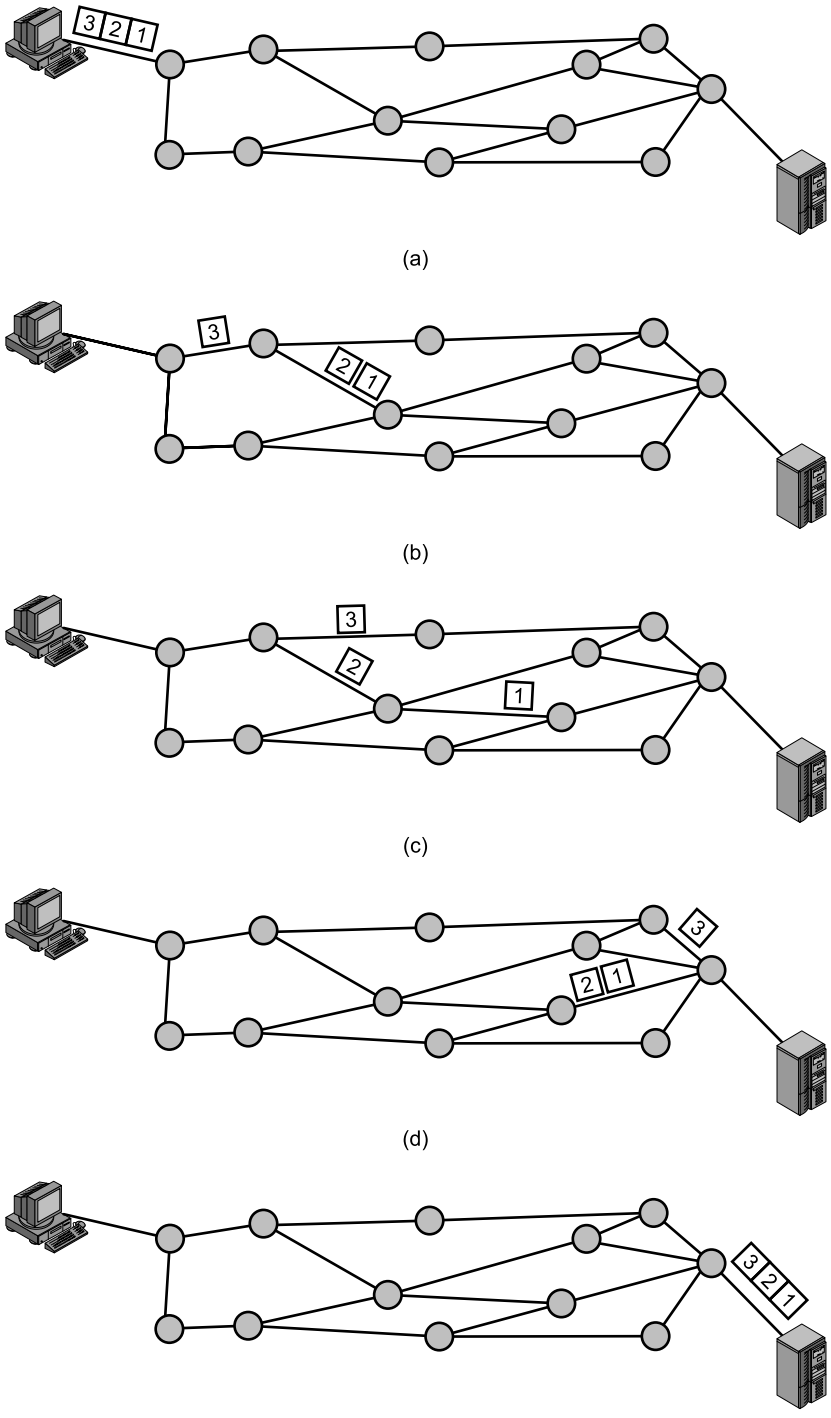


Figura 10.12. Conmutación de paquetes mediante datagramas.

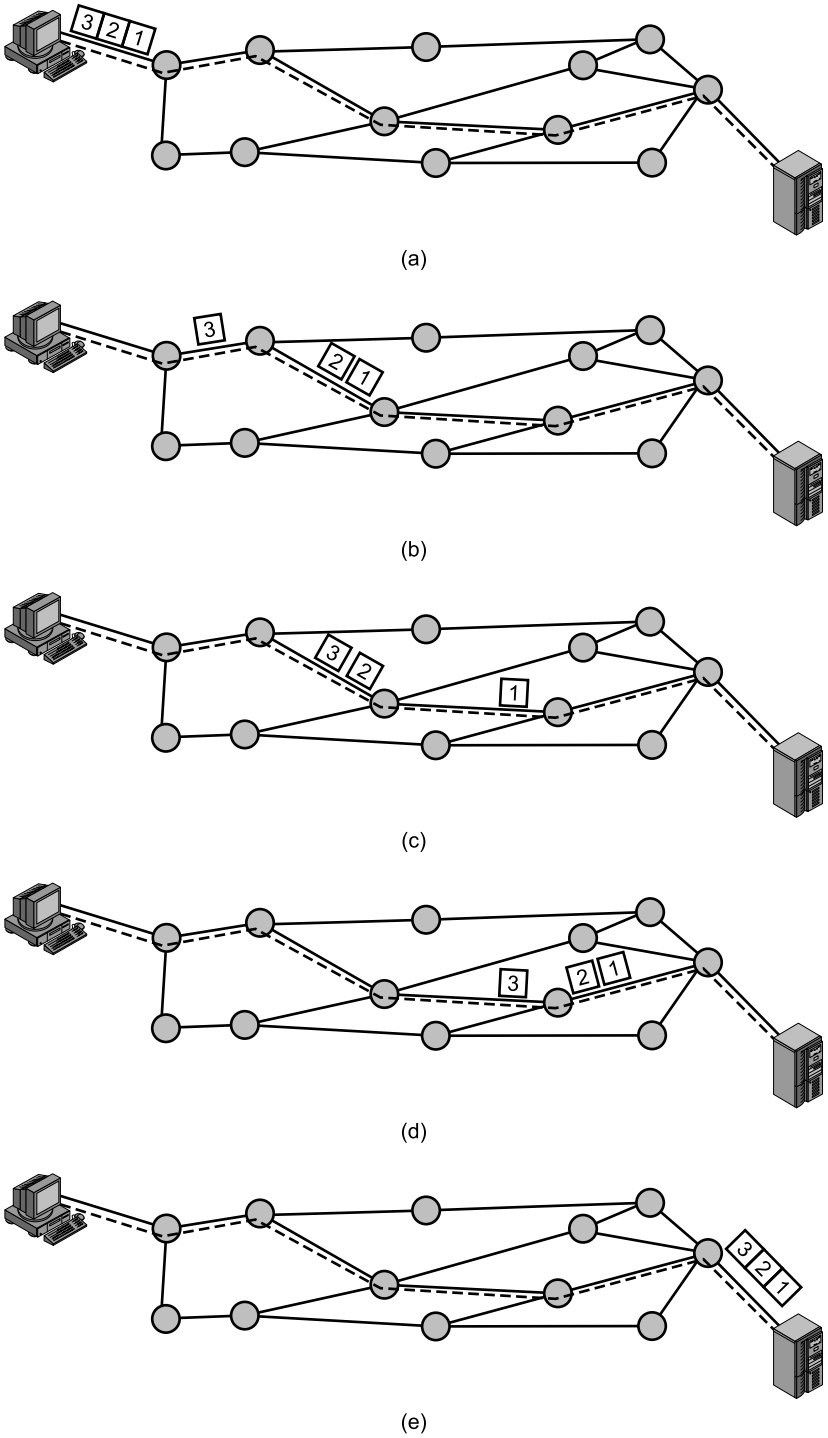


Figura 10.13. Conmutación de paquetes mediante circuitos virtuales.

retransmitirlos al destino. En algunas redes de datagramas es el destino final, en lugar del nodo, el responsable de llevar a cabo la reordenación de los paquetes. También es posible que los paquetes se pierdan en la red; por ejemplo, si un nodo de conmutación de paquetes falla momentáneamente, se perderán todos los paquetes en su cola. De nuevo, será responsabilidad del nodo final o del destino detectar la pérdida de un paquete y decidir cómo recuperarlo. En esta técnica, cada paquete se denomina datagrama y se trata de forma independiente del resto.

En la técnica de **circuitos virtuales** se establece una ruta previa al envío de los paquetes. Una vez establecida ésta, todos los paquetes intercambiados entre dos partes comunicantes siguen dicho camino a través de la red. Esto se ilustra en la Figura 10.13. Dado que el camino es fijo mientras dura la conexión lógica, éste es similar a un circuito en redes de conmutación de circuitos, por lo que se le llama circuito virtual. Además de los datos, cada paquete contiene un identificador de circuito virtual. Cada nodo de la ruta preestablecida sabe hacia dónde dirigir los paquetes, no precisándose por tanto la toma de decisiones de encaminamiento. En un instante de tiempo dado, cada estación puede tener más de un circuito virtual hacia otra u otras estaciones.

La principal característica de la técnica de circuitos virtuales es que la ruta entre las estaciones se establece antes de la transferencia de los datos. Obsérvese que esto no significa que sea una ruta dedicada como en el caso de la conmutación de circuitos. Un paquete continúa siendo almacenado en cada nodo y puesto en cola sobre una línea de salida, mientras que otros paquetes en otros circuitos virtuales pueden compartir el uso de la línea. La diferencia con la técnica de datagramas es que, en circuitos virtuales, el nodo no necesita tomar decisiones de encaminamiento para cada paquete, sino que ésta se toma una sola vez para todos los paquetes que usan dicho circuito virtual.

Si dos estaciones desean intercambiar datos durante un periodo de tiempo largo, existen ciertas ventajas al utilizar la técnica de circuitos virtuales. En primer lugar, la red puede ofrecer servicios sobre el circuito virtual, incluyendo orden secuencial y control de errores. El orden secuencial hace referencia al hecho de que, dado que los paquetes siguen la misma ruta, éstos se reciben en el mismo orden en que fueron enviados. El control de errores es un servicio que asegura que los paquetes no sólo se reciben en orden, sino que además son correctos. Por ejemplo, si un paquete en una secuencia del nodo 4 al 6 no llega a este último, o se recibe erróneamente, el nodo 6 puede solicitar al nodo 4 la retransmisión del paquete. Otra ventaja es que los paquetes viajan por la red más rápidamente haciendo uso de circuitos virtuales, ya que no es necesaria una decisión de encaminamiento para cada paquete en cada nodo.

Una ventaja del empleo de la técnica de datagramas es que no existe la fase de establecimiento de llamada. De esta forma, si una estación desea enviar sólo uno o pocos paquetes, el envío resultará más rápido. Otra ventaja del servicio datagrama es que, dado que es más rudimentario, resulta más flexible. Por ejemplo, si se produce congestión en una parte de la red, los datagramas entrantes se pueden encaminar siguiendo rutas lejanas a la zona de congestión. En cambio, en la técnica de circuitos virtuales los paquetes siguen una ruta predefinida, por lo que es más difícil para la red solucionar la congestión. Una tercera ventaja es que el envío datagrama es inherentemente más seguro. Con la utilización de circuitos virtuales, si un nodo falla se perderán todos los circuitos virtuales que atraviesan ese nodo. Por el contrario, en el envío datagrama, si un nodo falla los paquetes siguientes pueden encontrar una ruta alternativa que no atraviese dicho nodo. Como se verá en la Parte V del texto, en la interconexión de redes es usual el funcionamiento basado en datagramas.

TAMAÑO DE PAQUETE

Como se muestra en la Figura 10.14, existe una relación importante entre el tamaño de paquete considerado y el tiempo de transmisión. En este ejemplo se supone que existe un circuito virtual

desde la estación X a la estación Y a través de los nodos *a* y *b*. El mensaje a enviar es de 40 octetos y cada paquete contiene 3 octetos de información de control situada al comienzo del mismo y denominada cabecera. Si el mensaje completo se envía como un único paquete de 43 octetos (3 de cabecera y 40 octetos de datos), éste se envía primero desde la estación X hasta el nodo *a* (*véase* Figura 10.14a). Cuando se recibe el paquete completo, éste se puede transmitir de *a* a *b*. A su vez, cuando el paquete se recibe en *b*, se transfiere a la estación Y. Despreciando el tiempo de conmutación, el tiempo total de transmisión es de 129 veces el tiempo de duración de un octeto (43 octetos × 3 transmisiones del paquete).

Supongamos ahora que el mensaje se fragmenta en dos paquetes, cada uno con 20 octetos de mensaje y, claro está, 3 octetos de cabecera o información de control. En este caso, el nodo *a* puede comenzar a transmitir el primer paquete tan pronto como se reciba desde X, sin esperar al se

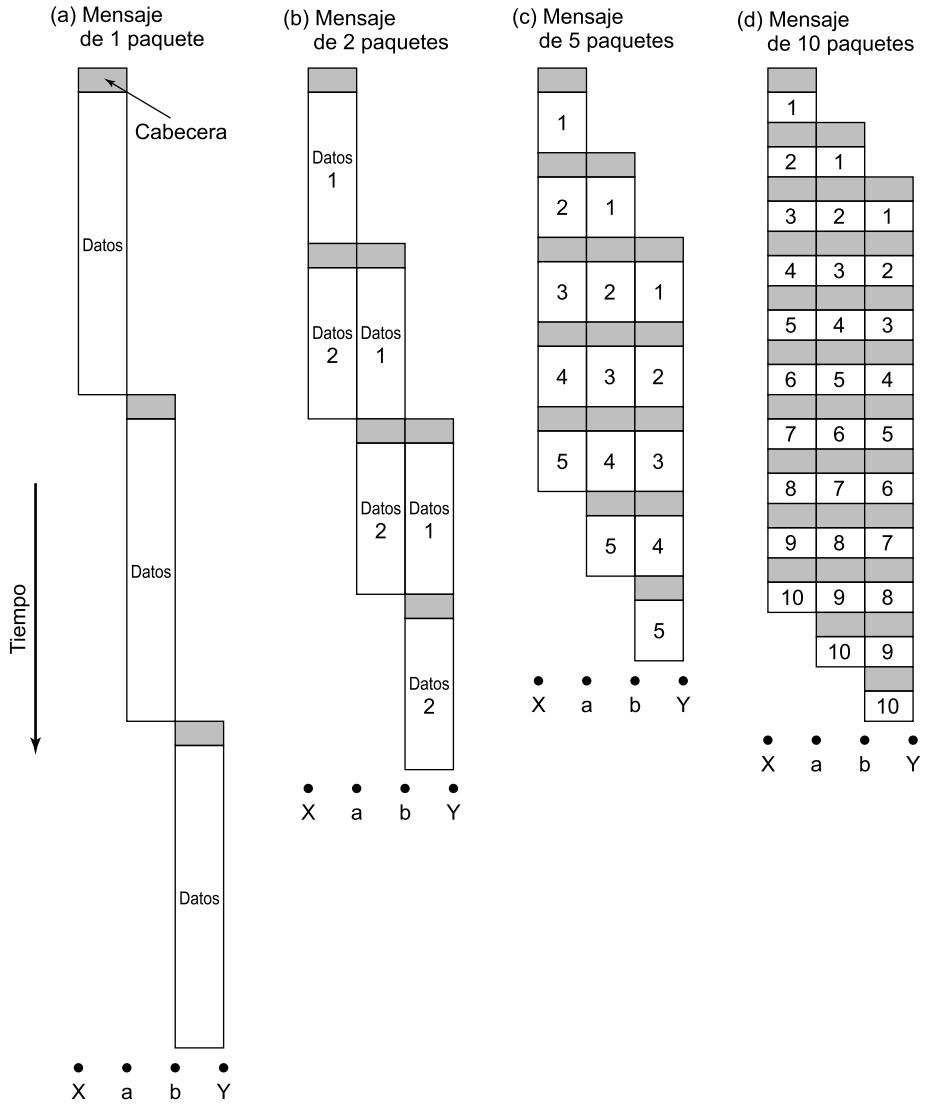


Figura 10.14. Efecto del tamaño de paquete en el tiempo de transmisión.

gundo paquete. Debido a este solapamiento en la transmisión, el tiempo total de ésta disminuye hasta 92 veces el tiempo de duración de un octeto. Troceando el mensaje en cinco paquetes, cada nodo intermedio puede comenzar la transmisión antes incluso, resultando superior el ahorro temporal conseguido: un total de 77 veces el tiempo de duración de un octeto. Sin embargo, tal y como se ilustra en la Figura 10.14d, el proceso de usar un número de paquetes mayor y de tamaño más pequeño puede provocar un incremento, en lugar de una reducción, en el retardo. Esto se debe a que cada paquete contiene una cantidad fija de datos de cabecera, y la existencia de más paquetes implica más cabeceras. Además, el ejemplo no muestra los retardos de procesamiento y puesta en cola en cada nodo, los cuales son también mayores cuantos más paquetes se usen para un mensaje dado. Sin embargo, veremos en el próximo capítulo que un tamaño de paquete excesivamente pequeño (53 octetos) puede dar lugar a un diseño de red eficiente.

COMPARACIÓN DE LAS TÉCNICAS DE CONMUTACIÓN DE CIRCUITOS Y DE PAQUETES

Una vez visto el funcionamiento interno de la técnica de conmutación de paquetes, a continuación se realizará una comparación de ella con la de conmutación de circuitos. En primer lugar nos centraremos en las prestaciones, examinándose posteriormente otras características.

Prestaciones

En la Figura 10.15 se muestra una comparación sencilla entre la conmutación de circuitos y las dos formas de conmutación de paquetes. Esta figura ilustra la transmisión de un mensaje a través de cuatro nodos, desde una estación emisora conectada al nodo 1 hasta una estación de destino conectada al nodo 4. En esta figura se indican tres tipos de retardo:

- **Retardo de propagación:** tiempo que tarda la señal en propagarse desde un nodo hasta el siguiente. Este tiempo es generalmente despreciable, ya que la velocidad de las señales electromagnéticas a través de un cable, por ejemplo, es generalmente de 2×10^8 m/s.
- **Tiempo de transmisión:** tiempo que tarda un transmisor en enviar un bloque de datos. Por ejemplo, en una línea de 10 kbps se tarda 1 segundo en transmitir un bloque de datos de 10.000 bits.
- **Retardo de nodo:** tiempo que tarda un nodo en realizar los procesos necesarios para la conmutación de los datos.

En conmutación de circuitos existe un cierto retardo antes de que se pueda enviar el mensaje. Primero se envía a través de la red una señal «Petición de Llamada» (*Call Request*) para establecer una conexión con el destino. Si la estación de destino no está ocupada, devuelve una señal «Llamada Aceptada» (*Call Accepted*). Obsérvese la aparición de un retardo de procesamiento en cada nodo durante la solicitud de llamada debido a la necesidad de establecer la ruta para la conexión. A la vuelta no se requiere procesamiento dado que la conexión está ya establecida. Una vez establecida la conexión, el mensaje se envía como un único bloque, sin retardos en los nodos de conmutación.

La técnica de conmutación de paquetes mediante circuitos virtuales parece muy similar a la de conmutación de circuitos. Un circuito virtual se solicita mediante el uso de un paquete «Petición de Llamada» (*Call Request*), el cual sufre un retardo en cada nodo. El circuito virtual se acepta mediante un paquete «Aceptación de Llamada» (*Call Accept*). Al contrario que en el caso de conmutación de circuitos, la aceptación de llamada también experimenta retardos en los nodos aunque

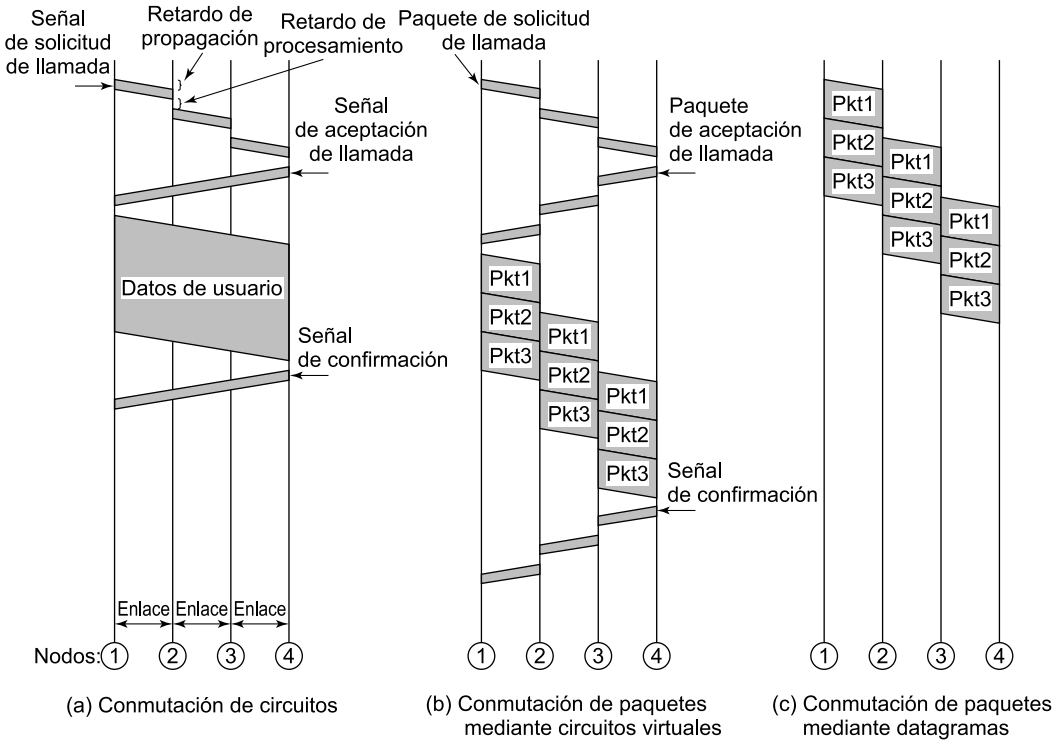


Figura 10.15. Eventos temporales en conmutación de circuitos y en conmutación de paquetes.

la ruta del circuito virtual se encuentre ya establecida. La razón de ello es que el paquete se pone en cola en cada nodo y debe esperar turno para su transmisión. Una vez establecido el circuito virtual, el mensaje se transmite en paquetes. Debería quedar claro que esta operación no puede ser más rápida, para redes comparables, que en el caso de la conmutación de circuitos. Este hecho se debe a que la conmutación de circuitos es, esencialmente, un proceso transparente, proporcionándose una velocidad de datos constante a través de la red. En cambio, la conmutación de paquetes involucra cierto retardo en cada nodo de la ruta; peor aún, este retardo es variable y aumenta con la carga.

La técnica de conmutación de paquetes mediante datagramas no precisa un establecimiento de llamada, de modo que para mensajes cortos resulta más rápida que la conmutación de paquetes mediante circuitos virtuales y, quizá, que la conmutación de circuitos. Sin embargo, dado que cada datagrama individual se encamina de forma independiente, el procesamiento de cada uno de ellos en cada nodo puede llegar a ser superior que en el caso de circuitos virtuales. Por tanto, para mensajes grandes, la técnica de circuitos virtuales puede ser mejor.

A partir de la Figura 10.15 se pueden comprender aproximadamente las prestaciones relativas de las distintas técnicas. Las prestaciones reales dependen de varios factores como el tamaño de la red, su topología, la carga y las características típicas de intercambios.

Otras características

Además de las prestaciones, existen numerosas características adicionales que se pueden tomar en consideración para llevar a cabo la comparación de las técnicas estudiadas. En la Tabla 10.2 se

resumen las más importantes. Aunque algunas de ellas ya se han visto, a continuación se presentan unos breves comentarios adicionales.

Tabla 10.2. Comparación de las técnicas de conmutación empleadas en comunicaciones.

Conmutación de circuitos	Conmutación de paquetes mediante datagramas	Conmutación de paquetes mediante circuitos virtuales
Ruta de transmisión dedicada	Ruta no dedicada	Ruta no dedicada
Transmisión de datos continua	Transmisión de paquetes	Transmisión de paquetes
Suficientemente rápida para aplicaciones interactivas	Suficientemente rápida para aplicaciones interactivas	Suficientemente rápida para aplicaciones interactivas
Los mensajes no se almacenan	Los paquetes se pueden almacenar hasta su envío	Los paquetes se almacenan hasta su envío
La ruta se establece para toda la conversación	La ruta se establece para cada paquete	La ruta se establece para toda la conversación
Existe retardo de establecimiento de la llamada; el retardo de transmisión es despreciable	Retardo en la transmisión de los paquetes	Existe retardo de establecimiento de llamada y de transmisión de los paquetes
Uso de señal de ocupado si el destino está ocupado	Se puede notificar al emisor acerca de que un paquete no se ha enviado	Se notifica al emisor sobre la denegación de conexión
La sobrecarga puede bloquear el establecimiento de la llamada; no existe retardo en las llamadas ya establecidas	La sobrecarga aumenta el retardo de paquete	La sobrecarga puede bloquear el establecimiento de la llamada; aumenta el retardo de paquete
Nodos de conmutación electromecánicos o computerizados	Nodos de conmutación pequeños	Nodos de conmutación pequeños
El usuario es el responsable de la protección ante pérdidas del mensaje	La red puede ser la responsable de paquetes individuales	La red puede ser la responsable de secuencias de paquetes
No existe generalmente conversión de velocidad ni de código	Existe conversión de velocidad y de código	Existe conversión de velocidad y de código
Ancho de banda fijo	Uso dinámico del ancho de banda	Uso dinámico del ancho de banda
No existen bits suplementarios tras el establecimiento de la llamada	Uso de bits suplementarios en cada paquete	Uso de bits suplementarios en cada paquete

Como se ha mencionado, la conmutación de circuitos es esencialmente un servicio transparente. Una vez que la conexión se ha establecido, se ofrece a las estaciones conectadas una velocidad de datos constante. Éste no es el caso de la conmutación de paquetes, en donde aparece generalmente un retardo variable y, en consecuencia, los datos no se reciben de forma constante. Además, en conmutación de paquetes mediante datagramas los datos pueden llegar en orden diferente al que fueron enviados.

Una consecuencia adicional de la transparencia es que no se precisa un coste extra para proveer de conmutación de circuitos. Una vez que se ha establecido la conexión, los datos analógicos o digitales van desde el origen hasta el destino. En conmutación de paquetes, los datos analógicos deben convertirse a digital antes de su transmisión; además, cada paquete incluye bits suplementarios relativos, por ejemplo, a la dirección de destino.

10.7. X.25

Aún queda por estudiar un aspecto de las redes de conmutación de paquetes: la interfaz entre los dispositivos conectados y la red. Ya se ha visto que las redes de conmutación de circuitos proporcionan una ruta de comunicación transparente para los dispositivos conectados, de tal modo que parece como si entre ellos existiese un enlace directo. Sin embargo, en el caso de las redes de conmutación de paquetes las estaciones conectadas deben organizar sus datos en paquetes para su transmisión. Esto requiere cierto grado de cooperación entre la red y las estaciones, cooperación definida en una norma de interfaz. El estándar usado casi universalmente con este fin es X.25.

X.25 es un estándar de ITU-T que especifica una interfaz entre una estación y una red de conmutación de paquetes. La funcionalidad de X.25 se especifica en tres niveles:

- Capa física.
- Capa de enlace.
- Capa o nivel de paquete.

La capa física trata la interfaz física entre una estación (computador, terminal) y el enlace que la conecta con un nodo de conmutación de paquetes. En el estándar se especifica la capa física en base a la norma conocida como X.21, aunque en muchos casos se utilizan otros estándares como el EIA-232. La capa de enlace se encarga de la transferencia fiable de datos a través del enlace físico mediante la transmisión de los datos como una secuencia de tramas. La capa de enlace estándar es el conocido como LAPB (protocolo balanceado de acceso al enlace, del inglés *Link Access Protocol Balanced*), el cual es un subconjunto del protocolo HDLC, descrito en el Capítulo 7.

El nivel de paquete proporciona un servicio de circuito virtual, lo que posibilita a un abonado de la red establecer conexiones lógicas, llamadas circuitos virtuales, con otros abonados. Un ejemplo de esto se muestra en la Figura 10.16 (compárese con la Figura 10.1). En este ejemplo, la estación A tiene una conexión de tipo circuito virtual con C; la estación B tiene establecidos dos circuitos virtuales, uno con C y otro con D; y cada una de las estaciones E y F mantiene un circuito virtual con D.

En este contexto, el término *circuito virtual* se refiere a la conexión lógica entre dos estaciones a través de la red; a esto se le suele denominar circuito virtual externo. Con anterioridad, utilizamos el término *circuito virtual* para referirnos a una ruta específica predefinida a través de la red entre dos estaciones; es el denominado circuito virtual interno. Generalmente, existe una relación uno a uno entre los circuitos virtuales internos y externos. Sin embargo, también es posible utilizar X.25 en una red de tipo datagrama. Lo importante en un circuito virtual externo es que se establece una relación lógica, o canal lógico, entre dos estaciones, considerándose todos los datos asociados a dicho canal lógico parte de una única secuencia de datos entre las estaciones. Por ejemplo, en la Figura 10.16, la estación D mantiene información acerca de los paquetes de datos recibidos de tres estaciones distintas (B, E, F) en base al número de circuito virtual asociado a cada paquete entrante.

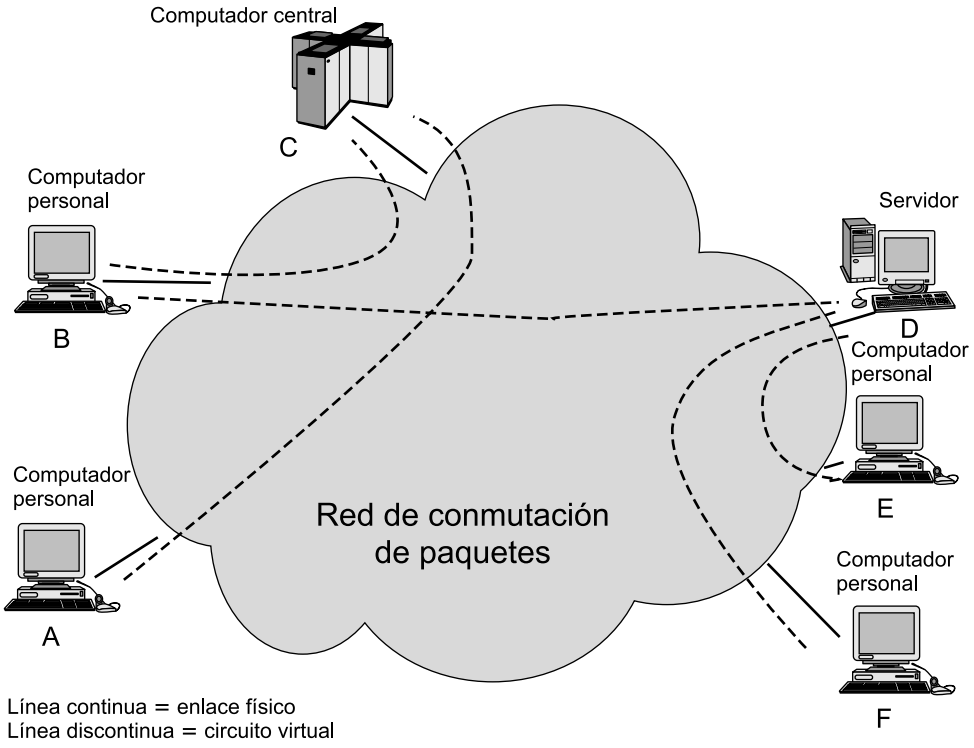


Figura 10.16. Ejemplo de utilización de circuitos virtuales.

En la Figura 10.17 se ilustra la relación entre las capas de X.25. Los datos de usuario se pasan hacia abajo al nivel 3 de X.25, el cual les añade una cabecera consistente en información de control, dando lugar a un paquete. Esta información de control tiene varios objetivos, entre los que se encuentran los siguientes:

1. Identificación de un circuito virtual dado mediante un número al que se asociarán los datos.
2. Definición de números de secuencia para su uso en el control de flujo y de errores sobre los circuitos virtuales.

Figura 10.17. Datos de usuario e información de control del protocolo X.25.

El paquete X.25 completo se pasa después a la entidad LAPB, que añade información de control al principio y al final del paquete, dando lugar a una trama LAPB (*véase* Figura 7.7). De nuevo, esta información de control en la trama es necesaria para el funcionamiento del protocolo LAPB.

El funcionamiento del nivel de paquete X.25 es similar al de HDLC, descrito en el Capítulo 7. Cada paquete de datos X.25 incluye números de secuencia de emisión y de recepción. El de emisión, P(S), se usa para numerar secuencialmente todos los paquetes de salida sobre un circuito virtual específico. El número de secuencia de recepción, P(R), es una confirmación de los paquetes recibidos sobre el circuito virtual en cuestión.

10.8. RETRANSMISIÓN DE TRAMAS

La técnica de retransmisión de tramas (*frame relay*) se diseñó para proporcionar un esquema de transmisión más eficiente que el proporcionado por X.25. Tanto las normalizaciones como los productos comerciales relacionados con la retransmisión de tramas aparecieron antes que los correspondientes a ATM, por lo que existe una amplia base de productos de retransmisión de tramas instalados. Es por ello que, a pesar del desplazamiento sufrido por esta técnica como consecuencia del interés actual por las redes de alta velocidad ATM, en esta sección se presenta una revisión de la retransmisión de tramas.

FUNDAMENTOS

La aproximación tradicional de conmutación de paquetes hace uso de X.25, lo que no sólo determina la interfaz usuario-red, sino que también afecta al diseño interno de la red. Algunas de las características básicas de X.25 son:

- Los paquetes de control de llamada, usados para el establecimiento y liberación de circuitos virtuales, se transmiten por el mismo canal y circuito virtual que los paquetes de datos, empleándose, en consecuencia, una señalización en banda.
- La multiplexación de circuitos virtuales tiene lugar en la capa 3.
- Tanto la capa 2 como la 3 incluyen mecanismos de control de flujo y de errores.

La aproximación X.25 es muy costosa, ya que el protocolo de control de enlace intercambia tramas de datos y de confirmación en cada salto a través de la red. Además, cada nodo intermedio debe mantener tablas de estado para cada circuito virtual con objeto de abordar aspectos de gestión de llamadas y de control de flujo/errores del protocolo X.25. Este coste queda justificado en caso de que la probabilidad de error en los enlaces de la red sea significativa, por lo que esta técnica puede no ser la más apropiada para los servicios de comunicación digitales modernos, dado que las redes actuales hacen uso de tecnologías de transmisión fiables sobre enlaces de transmisión de alta calidad, fibra óptica en muchos de los casos. Adicionalmente a este hecho, con la utilización de fibra óptica y transmisión digital se pueden conseguir velocidades de transmisión de datos elevadas. En este contexto, el coste de X.25 no sólo es innecesario, sino que además degrada la utilización efectiva de las altas velocidades de transmisión disponibles.

La retransmisión de tramas se ha diseñado para eliminar gran parte del coste que supone X.25 para el sistema final de usuario y para la red de conmutación de paquetes. Las principales diferencias entre la técnica de retransmisión de tramas y un servicio convencional de conmutación de paquetes X.25 son:

- La señalización de control de llamadas se transmite a través de una conexión lógica distinta de la de los datos de usuario. De este modo, los nodos intermedios no necesitan mantener tablas de estado ni procesar mensajes relacionados con el control de llamadas individuales.
- La multiplexación y conmutación de conexiones lógicas tienen lugar en la capa 2 en lugar de en la capa 3, eliminándose así una capa completa de procesamiento.
- No existe control de flujo ni de errores a nivel de líneas individuales (salto a salto). Si se lleva a cabo este control, será extremo a extremo y responsabilidad de capas superiores.

Así pues, en retransmisión de tramas sólo se envía una trama de datos de usuario desde el origen hasta el destino, devolviéndose al primero una trama de confirmación generada por una capa superior. En este caso no existe intercambio de tramas de datos y confirmaciones en cada uno de los enlaces del camino entre el origen y el destino.

Veamos las ventajas y desventajas que presenta esta técnica. En comparación con X.25, la principal desventaja teórica en retransmisión de tramas es que se pierde la posibilidad de llevar a cabo un control de flujo y de errores en cada enlace (aunque la retransmisión de tramas no ofrece control de flujo y de errores extremo a extremo, éste se puede implementar fácilmente en una capa superior). En X.25 existen varios circuitos virtuales a través de un mismo enlace físico, permitiendo el protocolo LAPB una transmisión fiable a nivel de enlace desde el origen hacia la red de conmutación de paquetes, y desde ésta hacia el destino. El protocolo de control de enlace proporciona, además, fiabilidad en cada enlace de la red. Con el uso de la técnica de retransmisión de tramas desaparece dicho control a nivel de enlace, aunque este hecho no supone un gran inconveniente gracias al incremento en la fiabilidad en la transmisión y en los servicios de conmutación.

La ventaja de la técnica de retransmisión de tramas es la potencia del proceso de comunicaciones, reduciéndose la funcionalidad del protocolo necesaria en la interfaz usuario-red así como el procesamiento interno de red. En consecuencia, cabe esperar un menor retardo y un mayor rendimiento. Así, algunos estudios indican que la mejora en el rendimiento mediante el uso de la técnica de retransmisión de tramas frente a X.25 puede ser de un orden de magnitud o más [HARB92]. La recomendación I.233 de ITU-T especifica que la retransmisión de tramas consigue velocidades de acceso de hasta 2 Mbps, si bien hay que decir que en la actualidad es posible alcanzar velocidades superiores.

ARQUITECTURA DE PROTOCOLOS EN RETRANSMISIÓN DE TRAMAS

En la Figura 10.18 se muestra la arquitectura de protocolos para proveer servicios de transporte en modo trama. Se consideran dos planos diferentes de operación: plano de control (C), relacionado con el establecimiento y liberación de conexiones lógicas, y plano de usuario (U), responsable de la transferencia de los datos de usuario entre abonados. Así, los protocolos del plano C se implementan entre el usuario y la red, mientras que los del plano U proveen de funcionalidad extremo a extremo.

Plano de control

El plano de control para servicios en modo trama es similar al de señalización por canal común para servicios de conmutación de circuitos por cuanto que se utiliza un canal lógico diferente para la información de control. En la capa de enlace se utiliza el protocolo LAPD (Q.921) para proporcionar un servicio de control del enlace de datos fiable, con control de errores y de flujo, entre el usuario (TE) y la red (NT) sobre el canal D. Este servicio de enlace de datos se usa para el intercambio de mensajes de señalización de control Q.933.

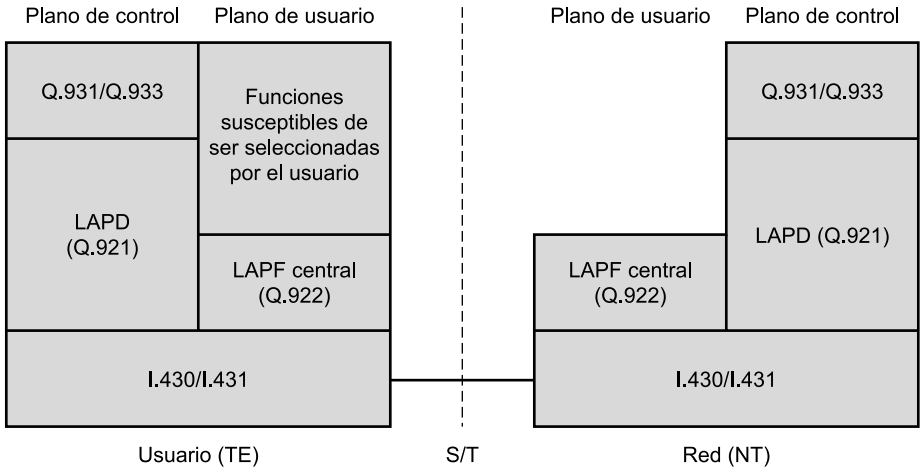


Figura 10.18. Arquitectura de protocolos en retransmisión de tramas para la interfaz usuario-red.

Plano de usuario

Definido en Q.922, LAPF (procedimiento de acceso al enlace para servicios en modo trama, *Link Access Procedure for Frame Mode Bearer Services*) es el protocolo del plano de usuario para la transferencia real de información entre usuarios finales. En retransmisión de tramas sólo se usan las funciones básicas de LAPF:

- Delimitación de tramas, alineamiento y transparencia.
- Multiplexación/demultiplexación de tramas utilizando el campo de dirección.
- Inspección de las tramas para asegurar que éstas constan de un número entero de octetos, antes de llevar a cabo la inserción de bits cero o tras una extracción de bits cero.
- Inspección de la trama para comprobar que no es demasiado larga ni demasiado corta.
- Detección de errores de transmisión.
- Funciones de control de congestión.

La última función es nueva en LAPF, siendo el resto funciones también presentes en LAPD.

Las funciones básicas de LAPF en el plano de usuario constituyen una subcapa de la capa del enlace de datos. Esto proporciona el servicio de transferencia de tramas del enlace de datos entre abonados sin control de flujo ni de errores. Además de este hecho, el usuario puede seleccionar funciones extremo a extremo adicionales de la capa de enlace o de la de red, las cuales no forman parte del servicio de retransmisión de tramas. De acuerdo con las funciones básicas, una red ofrece retransmisión de tramas como un servicio orientado a conexión de la capa de enlace con las siguientes propiedades:

- Se preserva el orden de la transferencia de tramas entre el origen y el destino.
- Existe una probabilidad pequeña de pérdida de tramas.

TRANSFERENCIA DE DATOS DE USUARIO

El funcionamiento de la técnica de retransmisión de tramas, por lo que respecta a la transferencia de datos de usuario, se explica mejor considerando el formato de trama, mostrado en la Figura 10.19a.

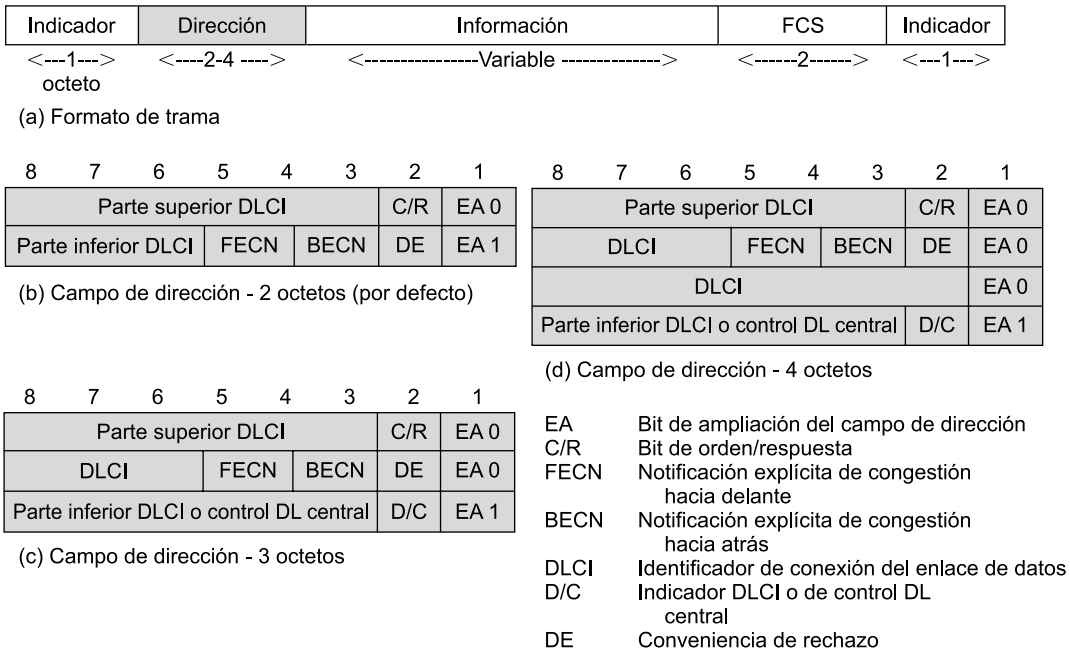


Figura 10.19. Formatos del protocolo central LAPF.

Éste es el formato definido para el protocolo LAPF de funcionalidad mínima (conocido como protocolo LAPF central), el cual es similar al de LAPD y LAPB con una salvedad obvia: no existe campo de control. Esto tiene las siguientes implicaciones:

- Existe un único tipo de trama, usada para el transporte de datos de usuario, y no existen tramas de control.
- No es posible el uso de señalización en banda; una conexión lógica sólo puede transmitir datos de usuario.
- No es posible llevar a cabo control de flujo ni de errores, dado que no existen números de secuencia.

Los campos indicador y secuencia de comprobación de trama (FCS) funcionan como en HDLC. El campo de información contiene datos de capas superiores, de modo que si el usuario decide implementar funciones adicionales de control del enlace de datos extremo a extremo, se puede incluir una trama de datos en este campo. En particular, una opción usual es el empleo del protocolo LAPF completo (conocido como protocolo LAPF de control) para llevar a cabo funciones por encima de las funciones centrales de LAPF. Obsérvese que el protocolo así implementado es estrictamente entre los abonados finales y resulta transparente para la red de retransmisión de tramas.

El campo de dirección tiene una longitud, por defecto, de 2 octetos, pudiéndose ampliar hasta 3 o 4 octetos. Este campo contiene un identificador de conexión del enlace de datos (DLCI, *Data Link Connection Identifier*) de 10, 16 o 23 bits. DLCI realiza la misma función que el número de circuito virtual en X.25: permite la multiplexación de varias conexiones lógicas de retransmisión de tramas a través de un único canal. Como en X.25, el identificador de conexión tiene sólo significado local: cada extremo de la conexión lógica asigna su propio DLCI de acuerdo con los números libres, debiendo realizar la red la conversión correspondiente entre ellos. Alternativamente, el

uso del mismo DLCI por parte de ambos extremos requeriría algún tipo de gestión global de los valores de DLCI.

La longitud del campo de dirección, y por tanto del DLCI, se determina mediante los bits de ampliación del campo de dirección (EA). El bit C/R es específico de la aplicación y no se usa en el protocolo de retransmisión de tramas estándar. Los bits restantes del campo de dirección están relacionados con el control de congestión y se discutirán en el Capítulo 13.

10.9. LECTURAS Y SITIOS WEB RECOMENDADOS

Como corresponde a su antigüedad, la conmutación de circuitos ha inspirado una voluminosa bibliografía. Dos buenos textos sobre este tema son [BELL00] y [FREE96]. En [BOSS98] y [FREE98] se trata la señalización de control. Por su parte, en [STAL99] se presenta en mayor detalle el protocolo SS7. Para un estudio en mayor profundidad de este protocolo resultan adecuados [BLAC97] y [RUSS95]. [BHAT97] proporciona también un tratamiento técnico detallado con especial énfasis en cuestiones de implementación práctica.

La bibliografía en torno a la conmutación de paquetes es muy extensa. Entre los libros que tratan adecuadamente este tema se encuentran [SPOH02], [BERT92] y [SPRA91].

Un estudio en mayor profundidad acerca de la técnica de retransmisión de tramas puede encontrarse en [STAL92], resultando [BUCK00] un excelente texto en este mismo campo.

BELL00 Bellamy, J. *Digital Telephony*. New York: Wiley, 2000.

BERT92 Bertsekas, D., y Gallager, R. *Data Networks*. Englewood Cliffs, NJ: Prentice Hall, 1992.

BHAT97 Bhatnagar, P. *Engineering Networks for Synchronization, CCS 7 and ISDN*. New York: IEEE Press, 1997.

BLAC97 Black, U. *ISDN and SS7: Architectures for Digital Signaling Networks*. Upper Saddle River, NJ: Prentice Hall, 1997.

BOSS98 Bosse, J. *Signaling in Telecommunication Networks*. New York: Wiley, 1998.

BUCK00 Buckwalter, J. *Frame Relay: Technology and Practice*. Reading, MA: Addison-Wesley, 2000.

FREE96 Freeman, R. *Telecommunication System Engineering*. New York: Wiley, 1996.

FREE98 Freeman, R. *Telecommunication Transmission Handbook*. New York: Wiley, 1998.

RUSS95 Russell, R. *Signaling System #7*. New York: McGraw-Hill, 1995.

SPOH02 Spohn, D. *Data Network Design*. New York: McGraw-Hill, 2002.

SPRA91 Spragins, J.; Hammond, J.; y Pawlikowski, K. *Telecommunications Protocols and Design*. Reading, MA: Addison-Wesley, 1991.

STAL99 Stallings, W. *ISDN and Broadband ISDN, with Frame Relay and ATM*. Upper Saddle River, NJ: Prentice Hall, 1999.

SITIOS WEB RECOMENDADOS

- **Consorcio internacional de *Softswitch*:** noticias, información técnica y comercial acerca de la tecnología y productos *softswitch*.
- **Grupo de trabajo de MGC:** puesto en marcha por la IETF para desarrollar el protocolo MGC (*Media Gateway Controller*) y estándares relacionados.
- **Foro de retransmisión de tramas:** asociación de vendedores, proveedores, usuarios y expertos para la implementación de la técnica de retransmisión de tramas de acuerdo con los estándares nacionales e internacionales. Este sitio incluye una lista de documentos técnicos y de implementación expuestos para su venta.
- **Centro de recursos de retransmisión de tramas:** buena fuente de información acerca de retransmisión de tramas.

10.10. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

abonado
bucle de abonado
bucle local
circuito virtual
conmutación de circuitos
conmutación de paquetes
conmutación por división en el espacio
conmutación por división en el tiempo
conmutador digital
conmutador lógico (*softswitch*)
controlador pasarela de medios (MGC)
datagrama
intercambio en modo no asociado
LAPB
LAPF
línea de abonado
línea troncal (*trunk*)
matriz de conexiones
modo asociado
punto de señalización
punto de transferencia de señal
red de conmutación de circuitos
retransmisión de tramas
señalización de control
señalización intrabanda (o en banda)
señalización fuera de banda
señalización intracanal
señalización por canal común
sistema de señalización número 7 (SS7)
X.25

CUESTIONES DE REPASO

10.1. ¿Por qué es útil disponer de más de una ruta a través de una red para cada pareja de estaciones?

10.2. ¿Cuáles son los cuatro componentes genéricos de la arquitectura de una red pública de comunicaciones? Defina cada uno de los términos.

10.3. ¿Cuál es la principal aplicación que ha primado en el diseño de las redes de conmutación de circuitos?

10.4. ¿Cuál es la diferencia entre la señalización intracanal y la de canal común?

10.5. ¿Cuáles son las ventajas de la técnica de conmutación de paquetes frente a la de conmutación de circuitos?

10.6. Explique las diferencias existentes entre el funcionamiento datagrama y el de circuitos virtuales.

10.7. ¿Cómo de importante es el tamaño de los paquetes en una red de conmutación de paquetes?

10.8. ¿Qué tipos de retardo son relevantes a la hora de calcular las prestaciones de una red de conmutación de paquetes?

10.9. ¿En qué se diferencia la técnica de retransmisión de tramas de la basada en X.25?

10.10. ¿Cuáles son las ventajas y desventajas relativas de retransmisión de tramas frente a X.25?

EJERCICIOS

10.1. Considere una red telefónica sencilla consistente en dos centrales finales y un conmutador intermedio con un enlace *full-duplex* de 1 MHz entre cada una de las centrales y el conmutador intermedio. Suponga un canal de 4 kHz para cada llamada de voz. La utilización media de cada teléfono es de cuatro llamadas cada 8 horas en horario comercial, con una duración media por llamada de seis minutos. El diez por ciento de las llamadas son de larga distancia. ¿Cuál es el número máximo de teléfonos que puede soportar cada central?

10.2. ¿Sería posible realizar una implementación de SS7 basada en conmutación de circuitos en lugar de en conmutación de paquetes? ¿Cuáles serían las ventajas relativas de esta aproximación?

10.3. Explique el punto débil del siguiente razonamiento: la conmutación de paquetes requiere que a cada paquete se le añadan bits de control y de dirección, lo que provoca un coste adicional en esta técnica. En conmutación de circuitos se establece un circuito transparente, no siendo necesario el uso de bits suplementarios. Por tanto, dado que no existe coste adicional en la técnica de conmutación de circuitos, la utilización de la línea es más eficiente que en conmutación de paquetes.

10.4. Se definen los siguientes parámetros para una red conmutada:

N = número de saltos entre dos sistemas finales dados

L = longitud del mensaje, en bits

B = velocidad de transmisión (en bps) de todos los enlaces

P = tamaño fijo del paquete, en bits

H = bits de redundancia o suplementarios (cabecera) por paquete

S = tiempo de establecimiento de llamada (conmutación de circuitos o circuitos virtuales) en segundos

D = retardo de propagación por salto, en segundos

a) Calcule el retardo extremo a extremo en conmutación de circuitos y en conmutación de paquetes mediante circuitos virtuales y mediante datagramas para $N = 4$, $L = 3.200$, $B = 9.600$, $P = 1.024$, $H = 16$, $S = 0{,}2$ y $D = 0{,}001$. Suponga que no se hace uso de confirmaciones e ignore el retardo de procesamiento en los nodos.

b) Obtenga las expresiones generales para las tres técnicas del apartado anterior, tomadas de dos en dos (tres expresiones en total), indicando las condiciones bajo las que el retardo es igual para todas ellas.

10.5. ¿Qué valor de P, como función de N, L y H, proporciona un retardo extremo a extremo mínimo en una red datagrama? Suponga que L es mucho mayor que P y $D = 0$.

10.6. Suponiendo que no se producen fallos en el funcionamiento de las estaciones ni de los nodos de una red, ¿es posible que un paquete se reciba en un destino incorrecto?

10.7. En las capas 2 y 3 de X.25 se usan procedimientos de control de flujo. ¿Son necesarios ambos o, por el contrario, son redundantes? Explíquelo.

10.8. En X.25 no existe mecanismo alguno de corrección de errores (secuencia de comprobación de trama). ¿No es necesario a fin de asegurar que todos los paquetes se reciban adecuadamente?

10.9. Dadas dos estaciones conectadas haciendo uso de X.25, ¿por qué es diferente el número de circuito virtual usado por cada una de ellas? Después de todo es el mismo circuito virtual *full-duplex*.

10.10. El documento Q.933 recomienda un procedimiento para llevar a cabo la negociación de la ventana de control de flujo mediante ventana deslizante, la cual puede tomar valores entre 1 y 127. Este proceso de negociación hace uso de la variable k, calculada mediante una expresión a partir de los siguientes parámetros:

L_d = tamaño de la trama de datos, en octetos

R_u = rendimiento, en bits/s

T_{td} = retardo de transmisión extremo a extremo, en segundos

k = tamaño de la ventana (número máximo de tramas I salientes)

El procedimiento es como sigue:

> El tamaño de la ventana se debe negociar como sigue. El usuario origen calcula k haciendo uso de la expresión mencionada, sustituyendo el retardo de transmisión extremo a extremo máximo y el tamaño máximo de trama de salida por T_{td} y L_d, respectivamente. El mensaje SETUP incluirá los parámetros del protocolo de la capa de enlace, los parámetros básicos de la capa de enlace y la información acerca del retardo de transmisión extremo a extremo. El usuario destino debe calcular su propio parámetro k haciendo uso de la expresión anterior, sustituyendo el retardo de transmisión extremo a extremo acumulado y su propio tamaño máximo de trama de salida por T_{td} y L_d, respectivamente. El mensaje CONNECT incluirá los parámetros básicos de la capa de enlace y la información acerca del retardo de transmisión extremo a extremo, de modo que el usuario origen puede modificar su parámetro k de acuerdo con esta información. El usuario origen debe calcular k haciendo uso de la expresión anterior, sustituyendo el retardo de transmisión extremo a extremo acumulado y el tamaño máximo de trama de entrada por T_{td} y L_d, respectivamente.

SETUP y CONNECT son mensajes intercambiados sobre un canal de control durante el establecimiento de una conexión de retransmisión de tramas. Sugiera una expresión para calcular k a partir de las otras variables y justifíquela.

CAPÍTULO 11

Modo de transferencia asíncrono

11.1. Arquitectura de protocolos

11.2. Conexiones lógicas ATM
Uso de conexiones de canal virtual
Características de camino virtual/canal virtual
Señalización de control

11.3. Celdas ATM
Formato de cabecera
Control de flujo genérico
Control de errores de cabecera

11.4. Transmisión de celdas ATM
Capa física basada en celdas
Capa física basada en SDH

11.5. Clases de servicios ATM
Servicios en tiempo real
Servicios en no tiempo real

11.6. Capa de adaptación ATM
Servicios AAL
Protocolos AAL

11.7. Lecturas y sitios web recomendados

11.8. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- ATM es una interfaz funcional de transferencia de paquetes que tienen un tamaño fijo y se denominan celdas. El uso de un tamaño y formato fijos hacen que esta técnica resulte eficiente para la transmisión a través de redes de alta velocidad.
- Para el transporte de celdas ATM debe usarse una estructura de transmisión. Una posibilidad consiste en la utilización de una cadena continua de celdas sin la existencia de una estructura de multiplexación de tramas en la interfaz; en este caso, la sincronización se lleva a cabo celda a celda. Una segunda opción es multiplexar las celdas mediante la técnica de división en el tiempo síncrona, en cuyo caso la secuencia de bits en la interfaz forma una trama externa basada en la jerarquía digital síncrona (SDH, *Synchronous Digital Hierarchy*).
- ATM proporciona servicios tanto en tiempo real como en no tiempo real, pudiendo soportar una amplia variedad de tipos de tráfico. Entre ellos cabe citar: secuencias TDM síncronas tales como T-1, usando el servicio de velocidad constante (CBR, *Constant Bit Rate*); voz y vídeo codificados, usando el servicio de velocidad variable en tiempo real (rt-VBR, *real-time Variable Bit Rate*); tráfico con requisitos específicos de calidad de servicio, usando el servicio en no tiempo real de velocidad variable (nrt-VBR, *non-real-time VBR*); y tráfico IP, haciendo uso de los servicios de velocidad disponible (ABR, *Available Bit Rate*), de velocidad sin especificar (UBR, *Unspecified Bit Rate*) y de velocidad de tramas garantizada (GFR, *Guaranteed Frame Rate*).
- El uso de ATM implica la necesidad de una capa de adaptación para aceptar protocolos de transferencia de información que no se encuentren basados en ATM. La capa de adaptación ATM (AAL, *ATM Adaptation Layer*) agrupa la información del usuario AAL en paquetes de 48 octetos y la encapsula en una celda ATM, lo que puede conllevar la agrupación de bits de una cadena o la segmentación de una trama en trozos más pequeños.

El modo de transferencia asíncrono (ATM, *Asynchronous Transfer Mode*), también conocido como retransmisión de celdas, aprovecha las características de fiabilidad y fidelidad de los servicios digitales modernos para proporcionar una conmutación de paquetes más rápida que X.25. ATM se desarrolló como parte del trabajo en RDSI de banda ancha, pero ha encontrado aplicación en entornos distintos de RDSI en los que se necesitan velocidades de transmisión muy elevadas.

En primer lugar se presenta una descripción detallada del esquema ATM. A continuación, se examinará el concepto de capa de adaptación ATM (AAL).

11.1. ARQUITECTURA DE PROTOCOLOS

El modo de transferencia asíncrono (ATM) es similar en muchos aspectos a la conmutación de paquetes usando X.25 y a la técnica de retransmisión de tramas. Como ellas, ATM lleva a cabo la transferencia de los datos en trozos discretos. Además, al igual que X.25 y retransmisión de tramas, ATM permite la multiplexación de varias conexiones lógicas a través de una única interfaz física. En el caso de ATM, el flujo de información en cada conexión lógica se organiza en paquetes de tamaño fijo denominados **celdas**.

ATM es un protocolo funcional con mínima capacidad de control de errores y de flujo, lo que reduce el coste de procesamiento de las celdas ATM y el número de bits suplementarios necesarios

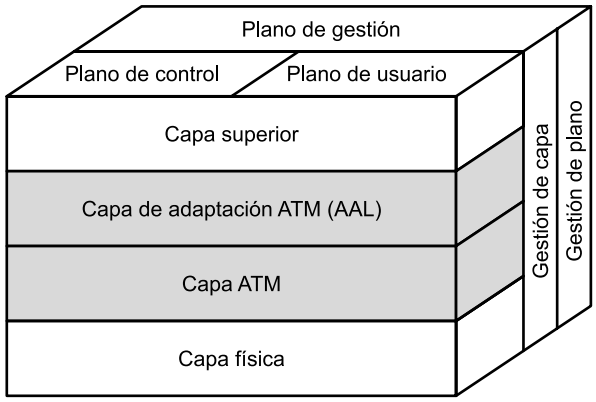


Figura 11.1. Arquitectura de protocolos ATM.

en cada celda, posibilitándose así su funcionamiento a altas velocidades. El uso de ATM a altas velocidades se ve apoyado adicionalmente por el empleo de celdas de tamaño fijo, ya que de este modo se simplifica el procesamiento necesario en cada nodo ATM.

Las normalizaciones de ITU-T para ATM se basan en la arquitectura de protocolos mostrada en el Figura 11.1, donde se ilustra la arquitectura básica para una interfaz entre un usuario y la red. La capa física contempla la especificación de un medio de transmisión y un esquema de codificación de señal. Las velocidades de transmisión especificadas en la capa física van desde 25,6 Mbps hasta 622,08 Mbps, siendo posibles velocidades superiores e inferiores.

Dos capas de la arquitectura de protocolos están relacionadas con las funciones ATM. Existe una capa ATM común a todos los servicios, que proporciona capacidad de transferencia de paquetes, y una capa de adaptación ATM (AAL, *ATM Adaptation Layer*), dependiente del servicio. La capa ATM define la transmisión de datos en celdas de tamaño fijo, al tiempo que establece el uso de conexiones lógicas. El empleo de ATM crea la necesidad de una capa de adaptación para dar soporte a protocolos de transferencia de información que no se fundamentan en ATM. AAL convierte la información procedente de capas superiores en celdas ATM para enviarlas a través de la red, al tiempo que extrae la información contenida en las celdas ATM y la transmite hacia las capas superiores.

El modelo de referencia de protocolos involucra tres planos independientes:

- **Plano de usuario:** permite la transferencia de información de usuario así como de controles asociados (por ejemplo, control de flujo y de errores).
- **Plano de control:** realiza funciones de control de llamada y de control de conexión.
- **Plano de gestión:** comprende la gestión de plano, que realiza funciones de gestión relacionadas con un sistema como un todo y proporciona la coordinación entre todos los planos, y la gestión de capa, que realiza funciones de gestión relativas a los recursos y a los parámetros residentes en las entidades de protocolo.

11.2. CONEXIONES LÓGICAS ATM

Las conexiones lógicas en ATM se denominan conexiones de canal virtual (VCC, *Virtual Channel Connection*). Una VCC es similar a un circuito virtual en X.25 y constituye la unidad básica de

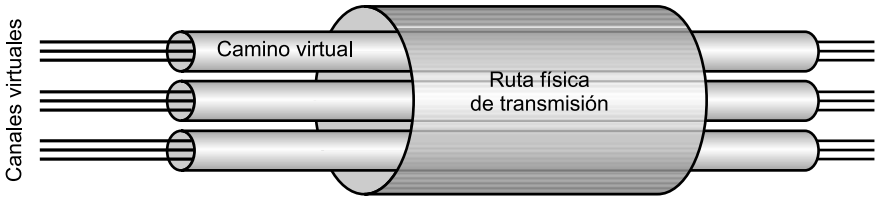


Figura 11.2. Relaciones entre conexiones ATM.

conmutación en una red ATM. Una VCC se establece a través de la red entre dos usuarios finales, intercambiándose sobre la conexión celdas de tamaño fijo en un flujo *full-duplex* de velocidad variable. Las VCC se utilizan también para intercambios usuario-red (señalización de control) y red-red (gestión de red y encaminamiento).

En ATM se ha introducido una segunda subcapa de procesamiento que gestiona el concepto de camino virtual (*véase* Figura 11.2). Una conexión de camino virtual (VPC, *Virtual Path Connection*) es un haz de VCC con los mismos extremos, de manera que todas las celdas transmitidas a través de todas las VCC de una misma VPC se conmutan conjuntamente.

El concepto de camino virtual se desarrolló en respuesta a una tendencia en redes de alta velocidad en la que el coste del control está alcanzando una proporción cada vez mayor del coste total de la red. La técnica de camino virtual ayuda a contener el coste asociado al control mediante la agrupación en una sola unidad de aquellas conexiones que comparten rutas comunes a través de la red. Las acciones de la gestión de red se pueden aplicar a un reducido número de grupos en lugar de a un número elevado de conexiones individuales.

El uso de los caminos virtuales presenta varias ventajas:

- **Arquitectura de red simplificada:** las funciones de transporte de la red se pueden dividir en dos grupos, aquellas relacionadas con una conexión lógica individual (canal virtual) y las relativas a un grupo de conexiones lógicas (camino virtual).
- **Incremento en la eficiencia y fiabilidad de red:** la red maneja entidades totales menores.
- **Reducción en el procesamiento y tiempo de establecimiento de conexión pequeño:** gran parte del trabajo se realiza cuando se establece el camino virtual, de modo que la reserva de capacidad en una VPC antes de la llegada de nuevas llamadas permite establecer nuevas VCC mediante la ejecución de funciones de control sencillas en los extremos del camino virtual. No se necesita procesamiento de llamadas en los nodos de tránsito, por lo que la incorporación de nuevos canales virtuales a un camino virtual ya existente implica un procesamiento mínimo.
- **Servicios de red mejorados:** el camino virtual se usa internamente a la red, aunque también es visible para el usuario final. Así, el usuario puede definir grupos de usuarios fijos o redes fijas de haces de canales virtuales.

En la Figura 11.3 se sugiere una forma general para el establecimiento de llamada haciendo uso de canales y caminos virtuales. El proceso de establecimiento de una VPC se encuentra desvinculado del proceso de establecimiento de una VCC individual:

- Entre los mecanismos de control de un camino virtual se encuentra la obtención de las rutas, la reserva de capacidad y el almacenamiento de información de estado de la conexión.
- El establecimiento de un canal virtual requiere la existencia previa de un camino virtual hacia el nodo de destino deseado, con suficiente capacidad disponible para dar cabida a dicho

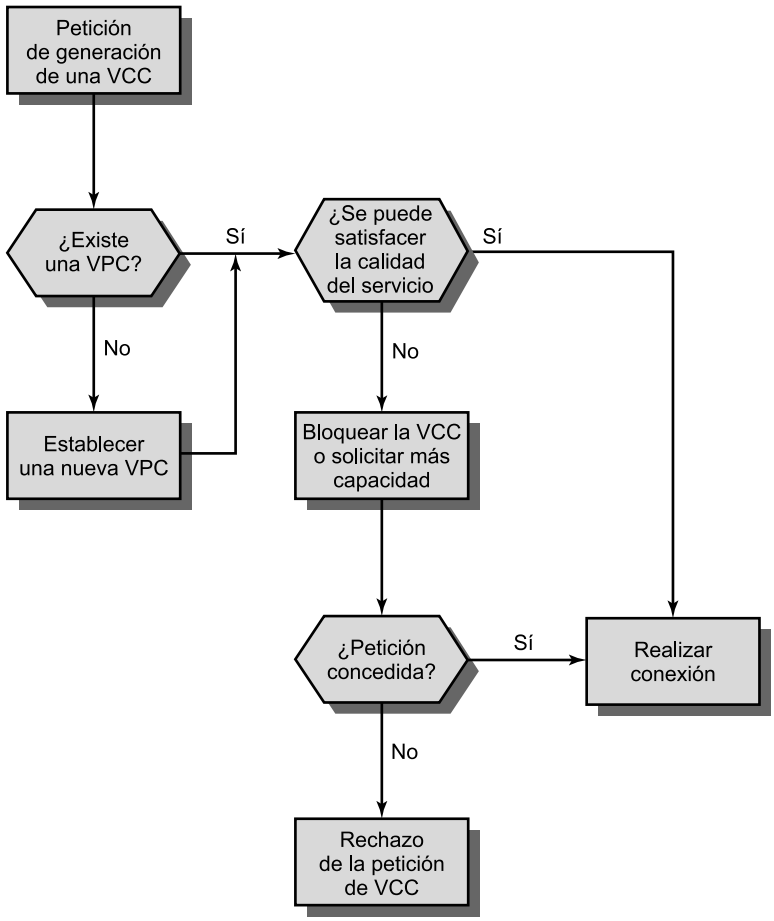


Figura 11.3. Establecimiento de llamadas mediante caminos virtuales.

canal virtual y con la calidad de servicio adecuada. El establecimiento se lleva a cabo mediante el almacenamiento de la información de estado necesaria (asociación canal virtual/camino virtual).

La terminología de caminos y canales virtuales usada en la normalización es un poco confusa, resumiéndose en la Tabla 11.1. Mientras que la mayoría de los protocolos de la capa de red tratados en este libro se refieren exclusivamente a la interfaz entre el usuario y la red, los conceptos de camino y canal virtual se definen en las recomendaciones ITU-T en relación a la interfaz usuario-red y al funcionamiento interno de la red.

USO DE CONEXIONES DE CANAL VIRTUAL

Los extremos de una VCC pueden ser usuarios finales, entidades de red o un usuario final y una entidad de red. En todos los casos se preserva la integridad de la secuencia de celdas dentro de una VCC; es decir, las celdas se entregan en el mismo orden en que se enviaron. Veamos ejemplos de los tres usos de una VCC:

Tabla 11.1. Terminología de camino virtual/canal virtual.

Canal virtual (VC)	Término genérico usado para describir el transporte unidireccional de celdas ATM asociadas a un valor identificador único común.
Enlace de canal virtual	Medio de transporte unidireccional de celdas ATM entre un punto al que se asigna un valor de VCI y el punto en que éste se traduce o termina.
Identificador de canal virtual (VCI)	Marca numérica única que identifica un enlace VC particular de una VPC dada.
Conexión de canal virtual (VCC)	Concatenación de enlaces VC que se extiende entre dos puntos donde los usuarios de servicio ATM acceden a la capa ATM. Las VCC se utilizan con fines de transferencia de información usuario-usuario, usuario-red o red-red. Se preserva la integridad de la secuencia de celdas para aquellas pertenecientes a la misma VCC.
Camino virtual	Término genérico usado para describir el transporte unidireccional de celdas ATM pertenecientes a canales virtuales asociados a un valor de identificación único común.
Enlace de camino virtual	Grupo de enlaces VC, identificado por un valor común de VPI, entre un punto al que se asigna un valor de VPI y el punto en que este valor se traduce o termina.
Identificador de camino virtual (VPI)	Identifica un enlace VP particular.
Conexión de camino virtual (VPC)	Concatenación de enlaces VP que se extiende entre el punto en que se asignan los valores de VCI y el punto en que estos valores se traducen o eliminan (es decir, amplía la longitud de un haz de enlaces VC que comparten el mismo VPI). Las VPC se emplean con objeto de transferir información usuario-usuario, usuario-red o red-red.

- **Entre usuarios finales:** se puede utilizar para el transporte extremo a extremo de datos de usuario y, como se verá más adelante, para la transmisión de señalización de control entre usuarios finales. Una VPC entre usuarios finales les concede a éstos una capacidad total; la organización de la VPC en VCC se utiliza por los dos usuarios finales siempre que el conjunto de las VCC no supere la capacidad de la VPC.
- **Entre un usuario final y una entidad de red:** se usa para la señalización de control desde el usuario hacia la red, como se verá posteriormente. Una VPC del usuario a la red se puede emplear para el tráfico total desde un usuario final hacia un conmutador o un servidor de red.
- **Entre dos entidades de red:** utilizado para la gestión del tráfico de red y para funciones de encaminamiento. Una VPC red-red puede ser usada para definir una ruta común para el intercambio de información de gestión de red.

CARACTERÍSTICAS DE CAMINO VIRTUAL/CANAL VIRTUAL

En la recomendación I.150 de la ITU-T se especifican las siguientes características para las conexiones de canal virtual:

- **Calidad de servicio:** un usuario de una VCC es provisto con una calidad de servicio especificada por parámetros como la tasa de pérdida de celdas (relación entre las celdas perdidas y las transmitidas) y la variación del retardo de celdas.

- **Conexiones de canal virtual conmutadas y semipermanentes:** una VCC conmutada es una conexión bajo demanda que necesita señalización de control de llamada para su establecimiento y terminación. Una VCC semipermanente se caracteriza por ser de larga duración y llevarse a cabo su establecimiento a través de una acción de configuración o de gestión de red.
- **Integridad de la secuencia de celdas:** se preserva la naturaleza secuencial de la cadena de celdas transmitida en una VCC.
- **Negociación de parámetros de tráfico y supervisión del uso:** entre un usuario y la red se pueden negociar parámetros de tráfico para cada VCC. La entrada de celdas a la VCC es supervisada por la red para asegurar que se cumplen los parámetros negociados.

Entre los tipos de parámetros de tráfico que se pueden negociar se encuentran la velocidad media, la velocidad de pico, la aparición de ráfagas y la duración de pico. La red puede necesitar la utilización de varias estrategias para tratar la congestión y gestionar tanto las VCC existentes como las solicitadas. Al nivel más básico, la red puede limitarse simplemente a denegar nuevas peticiones de VCC para prevenir la congestión. Adicionalmente, las celdas se pueden descartar si no se respetan los parámetros negociados o si la congestión llega a ser importante, pudiendo llegar a liberarse las conexiones existentes si la situación es extrema.

El documento I.150 especifica también características para las VPC. Las cuatro primeras son idénticas a las de las VCC; es decir, garantía de calidad de servicio, existencia de VPC conmutadas y semipermanentes, integridad de la secuencia de celdas y negociación de parámetros de tráfico y supervisión del uso son también características propias de una VPC. Existen varias razones para esta duplicidad. En primer lugar, se provee así de cierta flexibilidad sobre cómo el servicio de red gestiona los requisitos que debe cumplir. En segundo lugar, la red debe ocuparse de las necesidades de una VPC y, dentro de una VPC, puede negociar el establecimiento de canales virtuales con unas características concretas. Por último, una vez que se ha establecido una VPC, los usuarios finales pueden negociar la creación de nuevas VCC. Las características de una VPC determinan las elecciones que los usuarios finales pueden hacer.

Adicionalmente, existe una quinta característica para las VPC:

- **Restricción de identificador de canal virtual en una VPC:** puede que no sea posible proporcionar al usuario de una VPC uno o más identificadores, o números, de canal virtual, pero sí se pueden reservar para el uso de la red. Algunos ejemplos incluyen el uso de VCC para la gestión de la red.

SEÑALIZACIÓN DE CONTROL

En ATM es necesario un mecanismo para el establecimiento y liberación de VPC y VCC. El intercambio de información involucrado en este proceso se denomina señalización de control y tiene lugar a través de conexiones distintas de las que están siendo gestionadas.

El documento I.150 especifica cuatro métodos para llevar a cabo el establecimiento/liberación de VCC. En todas las redes se usa uno o una combinación de los siguientes métodos:

1. Las **VCC semipermanentes** se pueden usar para el intercambio usuario-usuario, en cuyo caso no se necesita señalización de control.
2. Si no existe canal de señalización de control de llamada preestablecido, se debe establecer uno. Con este fin debe tener lugar un intercambio de señales de control entre el usuario y la red a través de algún canal. Por tanto, es necesario un canal permanente, probablemente

de baja velocidad, que pueda ser utilizado para establecer las VCC usadas para el control de llamadas. Un canal de este tipo se denomina **canal de metaseñalización**, dado que se emplea para establecer canales de señalización.

3. El canal de meta-señalización se puede usar para establecer una VCC entre el usuario y la red para la señalización de control de llamadas. Este **canal virtual de señalización del usuario a la red** se puede utilizar para establecer VCC para la transmisión de datos de usuario.
4. El canal de meta-señalización se puede utilizar también para establecer un **canal virtual de señalización usuario-usuario**, que debe configurarse en una VPC preestablecida. Este canal se puede utilizar para posibilitar a los dos usuarios finales, sin que la red intervenga, el establecimiento y liberación de VCC usuario-usuario para el transporte de datos de usuario.

En I.150 se definen tres métodos para las VPC:

1. Una VPC se puede establecer de forma **semipermanente** con negociación previa. En este caso no se necesita señalización de control.
2. El establecimiento/liberación de las VPC puede ser **controlado por el usuario**, en cuyo caso éste utiliza una VCC de señalización para solicitar la VPC a la red.
3. El establecimiento/liberación de las VPC puede ser **controlado por la red**. En este caso, la red establece una VPC para su propio uso, pudiendo ser el camino de tipo red-red, del usuario a la red o usuario-usuario.

11.3. CELDAS ATM

El modo de transferencia asíncrono hace uso de celdas de tamaño fijo, las cuales constan de 5 octetos de cabecera y de un campo de información de 48 octetos. El empleo de celdas pequeñas de tamaño fijo presenta varias ventajas. En primer lugar, puede reducir el retardo de cola para celdas de alta prioridad, ya que la espera es menor si se reciben ligeramente después de que una celda de baja prioridad haya conseguido el acceso a un recurso (por ejemplo, el transmisor). En segundo lugar, parece que las celdas de tamaño fijo se pueden conmutar más eficientemente, lo que es importante para las altas velocidades de ATM [PARE88]. La implementación hardware de los mecanismos de conmutación es más fácil para celdas de tamaño fijo.

FORMATO DE CABECERA

En la Figura 11.4a se muestra el formato de cabecera de las celdas en la interfaz usuario-red, mientras que en la Figura 11.4b se muestra el formato de cabecera de las celdas internas a la red.

El campo de **control de flujo genérico** (GFC, *Generic Flow Control*) no se incluye en la cabecera de las celdas internas a la red, sino sólo en la interfaz usuario-red, por lo que únicamente se puede usar para llevar a cabo el control de flujo de celdas en la interfaz local entre el usuario y la red. Este campo podría utilizarse para ayudar al usuario en el control del flujo de tráfico para diferentes calidades de servicio. En cualquier caso, el mecanismo GFC se usa con el fin de aliviar la aparición esporádica de sobrecarga en la red.

El documento I.150 especifica como requisito del mecanismo GFC que todos los terminales sean capaces de acceder a sus respectivas capacidades aseguradas. Esto incluye a todos los termi-

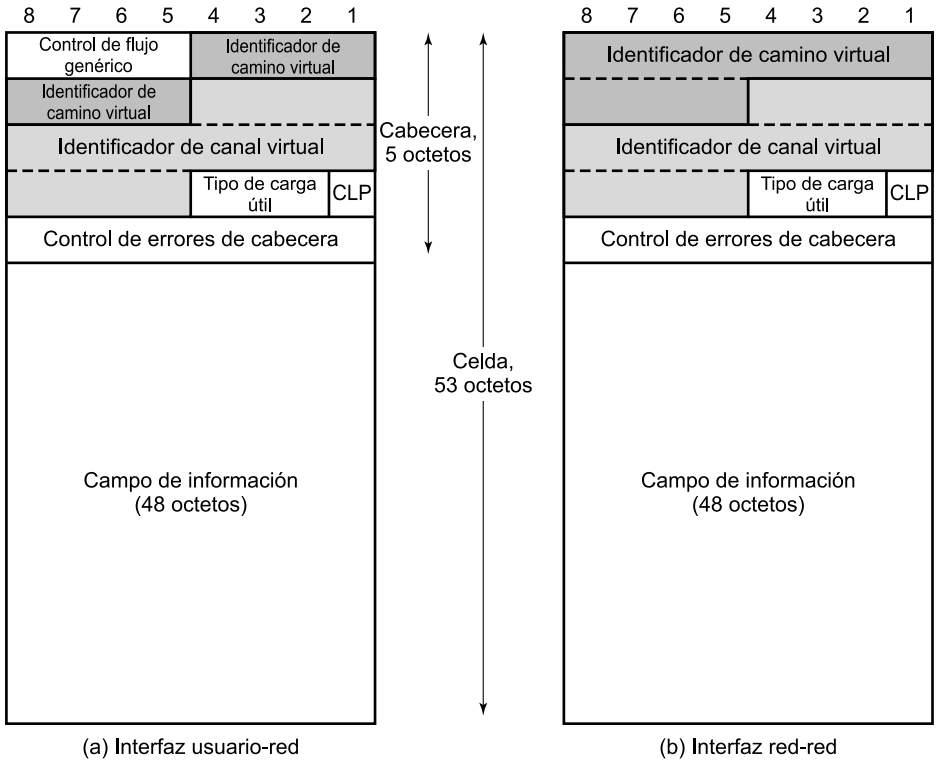

8 7 6 5 4 3 2 1
Control de flujo genérico
Identificador de camino virtual
Identificador de camino virtual
Identificador de canal virtual
Tipo de carga útil
CLP
Control de errores de cabecera
Campo de información (48 octetos)
Cabecera, 5 octetos
Celda, 53 octetos
(a) Interfaz usuario-red
8 7 6 5 4 3 2 1
Identificador de camino virtual
Identificador de canal virtual
Tipo de carga útil
CLP
Control de errores de cabecera
Campo de información (48 octetos)
(b) Interfaz red-red

Figura 11.4. Formato de celda ATM.

nales de velocidad constante (CBR, *Constant-Bit-Rate*) así como a los de velocidad variable (VBR, *Variable-Bit-Rate*) que disponen de un elemento de capacidad garantizada (CBR y VBR se explicarán en la Sección 11.5). El mecanismo GFC actual se describe en el siguiente apartado.

El **identificador de camino virtual** (VPI, *Virtual Path Identifier*) es un campo de encaminamiento para la red, de 8 bits para la interfaz usuario-red y de 12 bits para la interfaz red-red. Este último caso permite un número superior de VPC internas a la red, tanto para dar servicio a subscriptores como las necesarias para la gestión de red. El **identificador de canal virtual** (VCI, *Virtual Channel Identifier*) se emplea para encaminar a y desde el usuario final.

El campo **tipo de carga útil** (PT, *Payload Type*) indica el tipo de información contenida en el campo de información. En la Tabla 11.2 se muestra la interpretación de los bits PT. Un valor 0 en el primer bit indica información de usuario (es decir, información procedente de la capa inmediatamente superior). En este caso, el segundo bit indica si se ha producido o no congestión; el tercer bit, llamado tipo de unidad de datos de servicio (SDU)[1], es un campo de 1 bit que se puede usar para discriminar dos tipos de SDU ATM asociadas a una conexión dada. El término *SDU* se refiere a la carga útil de 48 octetos de la celda. Un valor 1 en el primer bit del campo PT indica que la celda transporta información de gestión de red o de mantenimiento. Esto permite la inserción de celdas de gestión de red en una VCC de usuario sin afectar a los datos de usuario, por lo que el campo PT puede proporcionar información de control intrabanda.

[1] Éste es el término utilizado en los documentos del Foro ATM. Por su parte, en los documentos de ITU-T se le denomina a este bit *bit de indicación usuario ATM-usuario ATM* (AAU). El significado es el mismo en ambos casos.

Tabla 11.2. Codificación del campo de tipo de carga útil (PT).

Codificación PT	Interpretación
0 0 0	Celda de datos de usuario, no se ha producido congestión, tipo de SDU = 0
0 0 1	Celda de datos de usuario, no se ha producido congestión, tipo de SDU = 1
0 1 0	Celda de datos de usuario, se ha producido congestión, tipo de SDU = 0
0 1 1	Celda de datos de usuario, se ha producido congestión, tipo de SDU = 1
1 0 0	Celda asociada a segmento OAM
1 0 1	Celda asociada a OAM extremo a extremo
1 1 0	Celda de gestión de recursos
1 1 1	Reservada para funciones futuras

SDU = Unidad de Datos de Servicio.
OAM = Funcionamiento, Administración y Mantenimiento.

El bit **prioridad de pérdida de celdas** (CLP, *Cell Loss Priority*) se emplea para ayudar a la red ante la aparición de congestión. Un valor 0 indica que la celda es de prioridad relativamente alta, no debiendo ser descartada a menos que no quede otra opción; un valor 1 indica, por el contrario, que la celda puede descartarse. El usuario puede utilizar este campo para insertar celdas extra en la red (una vez negociada la velocidad), con CLP igual a 1, y transmitirlas al destino si la red no está congestionada. La red puede poner este campo a 1 en aquellas celdas que violen los parámetros de tráfico acordados entre el usuario y la red. En este caso, el conmutador que lo activa se percata de que la celda excede los parámetros de tráfico establecidos pero que ésta puede ser procesada. Posteriormente, si se encuentra congestión en la red, esta celda se marcará para su rechazo antes que aquellas que se encuentran dentro de los límites de tráfico fijados.

Como se explica más adelante, el campo de **control de errores de cabecera** se usa tanto para el control de errores como con fines de sincronización.

CONTROL DE FLUJO GENÉRICO

En el documento I.150 se especifica el uso del campo GFC para llevar a cabo el control de flujo del tráfico en la interfaz usuario-red (UNI, *User-Network Interface*) con objeto de solucionar la aparición esporádica de sobrecarga. El mecanismo de control de flujo se define en el documento I.361: el control de flujo GFC forma parte de un mecanismo propuesto para la transferencia controlada de celdas (CCT, *Controlled Cell Transfer*), el cual está pensado para satisfacer los requisitos de redes LAN no ATM conectadas a una red ATM de área amplia [LUIN97]. En particular, el mecanismo CCT está ideado para ofrecer un buen servicio para tráfico a ráfagas elevado con mensajes de longitud variable. En el resto de este apartado se estudia el mecanismo GFC tal y como se especifica en la normalización.

Cuando los equipos en la UNI están configurados para aceptar el mecanismo GFC, se usan dos tipos de procedimientos: transmisión controlada y transmisión no controlada. Esencialmente, cada conexión se identifica como sujeta a control de flujo o como no sujeta a control de flujo. Para las primeras puede existir un grupo de conexiones controladas (grupo A), lo que constituye el caso por defecto, o el tráfico controlado se puede clasificar en dos grupos de conexiones controladas (grupo A y grupo B), las cuales se conocen como modelos de una cola y de dos colas, respectivamente. El control de flujo se lleva a cabo por parte de la red en la dirección desde el abonado hacia ella.

Considérese en primer lugar el funcionamiento del mecanismo GFC cuando sólo existe un grupo de conexiones controladas. El equipo controlado, llamado equipo terminal (TE, *Terminal Equipment*), inicializa el valor de dos variables: TRANSMIT, que es un bit de señalización y que

se hace igual a SET (1), y GO_CNTR, contador de créditos, que toma inicialmente el valor 0. Una tercera variable, GO_VALUE, se hace igual a 1 o un valor superior en el momento de la configuración. Las reglas de transmisión para el dispositivo controlado son las siguientes:

1. Si TRANSMIT = 1, se pueden enviar celdas en cualquier instante de tiempo sobre conexiones no controladas. Si TRANSMIT = 0, no se pueden enviar celdas ni sobre las conexiones controladas ni sobre las no controladas.

2. Si se recibe una señal HALT del equipo de control, se hace TRANSMIT igual a 0 y permanece a este valor hasta que se reciba una señal NO_HALT, en cuyo caso TRANSMIT pasará a valer 1.

3. Si TRANSMIT = 1 y no se dispone de celdas a transmitir sobre ninguna conexión no controlada:

   — Si GO_CNTR > 0, el TE puede enviar una celda sobre una conexión controlada. El TE marca esta celda como una celda de una conexión controlada y decrementa GO_CNTR.

   — Si GO_CNTR = 0, el TE no puede enviar una celda sobre una conexión controlada.

4. El TE hace GO_CNTR igual a GO_VALUE ante la recepción de una señal SET; una señal nula no tiene efecto sobre la variable GO_CNTR.

La señal HALT se usa para limitar lógicamente la velocidad ATM efectiva, debiendo ser de naturaleza cíclica. Por ejemplo, para reducir a la mitad la velocidad de un enlace, el equipo de control genera la orden HALT de forma que sea efectiva durante el 50% del tiempo. Esto se lleva a cabo de forma regular y predecible a lo largo de la duración de una conexión física.

En el modelo de dos colas existen dos contadores, cada uno de ellos con un valor actualizado y otro inicial: GO_CNTR_A, GO_VALUE_A, GO_CNTR_B y GO_VALUE_B. Esto permite al NT2 controlar dos grupos distintos de conexiones.

En la Tabla 11.3 se resumen las reglas de activación de los bits GFC.

Tabla 11.3. Codificación del campo de control de flujo genérico (GFC).

	No controlado	**Controlador → controlado**		**Controlado → controlador**	
		Modelo de 1 cola	**Modelo de 2 colas**	**Modelo de 1 cola**	**Modelo de 2 colas**
Primer bit	0	HALT(0)/ NO_HALT(1)	HALT(0)/ NO_HALT(1)	0	0
Segundo bit	0	SET(1)/ NULL(0)	SET(1)/ NULL(0) para el grupo A	Celda perteneciente a conexión controlada (1)/ no controlada (0)	Celda perteneciente (1)/ o no (0) al grupo A
Tercer bit	0	0	SET (1)/ NULL (0) para el grupo B	0	Celda perteneciente (1)/ o no (0) al grupo B
Cuarto bit	0	0	0	El equipo es no controlado (0)/controlado (1)	El equipo es no controlado (0)/controlado (1)

CONTROL DE ERRORES DE CABECERA

Cada celda ATM incluye un campo de control de errores de cabecera (HEC, *Header Error Control*), que se calcula en base a los restantes 32 bits de la cabecera. El polinomio usado para generar el código es $X^8 + X^2 + X + 1$. En la mayor parte de los protocolos existentes que incluyen un campo de control de errores, como es el caso de HDLC, la cantidad de datos de entrada para el cálculo del código de error es generalmente mayor que el tamaño del código de error resultante, lo que permite la detección de errores. En el caso de ATM, la entrada para el cálculo es sólo de 32 bits, frente a los 8 bits del código. El hecho de que la entrada sea relativamente pequeña permite el uso del código no sólo para la detección de errores, sino que, en algunos casos, es posible la corrección de éstos. Esto se debe a que hay suficiente redundancia en el código para recuperar ciertos patrones de error.

En la Figura 11.5 se muestra el funcionamiento del algoritmo HEC en el receptor. Inicialmente, el algoritmo de corrección de errores del receptor corrige implícitamente errores simples. Para cada celda recibida se calcula y compara el HEC. Si no se detectan errores, el receptor permanece en el modo de corrección de errores. En cambio, si se detecta un error, el receptor lo corrige si se trata de un error simple o, en caso contrario, detectará la ocurrencia de un error múltiple. En cualquier caso, el receptor pasa a modo de detección, no tratando de corregir errores. La razón de este cambio es que un ruido de tipo ráfaga u otro suceso podrían causar una secuencia de errores, situación para la que el HEC resulta insuficiente para su corrección. El receptor permanece en el modo de detección mientras se reciban celdas erróneas, pasando al modo de corrección cuando se examina una cabecera y no se encuentra error alguno. El diagrama de flujo de la Figura 11.6 muestra el efecto de la aparición de errores en la cabecera de una celda.

La función de protección de errores permite la recuperación de los errores de cabecera simples y la existencia de una baja probabilidad de envío de celdas con errores de cabecera provocados por situaciones de errores a ráfagas. Las características de error en sistemas de transmisión de fibra óptica parecen ser una mezcla de errores simples y errores a ráfagas relativamente largas. En algunos sistemas de transmisión no se utiliza la capacidad de detección de errores debido a su alto coste temporal.

En la Figura 11.7, basada en una que aparece en la recomendación I.432 de ITU-T, se indica la forma en que los errores en bits aleatorios afectan a la probabilidad de rechazo de celdas y a la obtención de celdas válidas con cabeceras erróneas cuando se usa HEC.

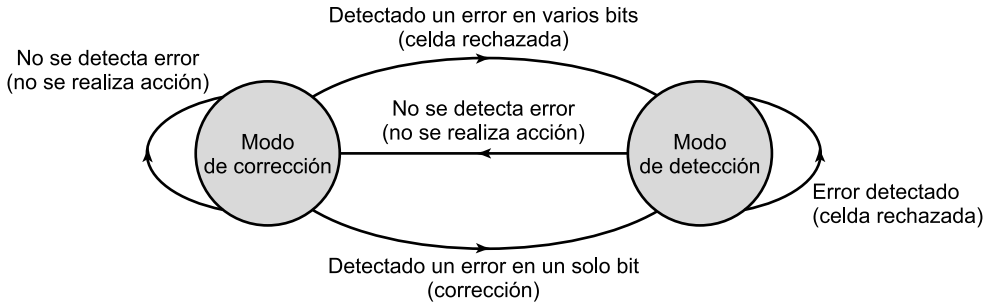


Figura 11.5. Operación HEC en el receptor.

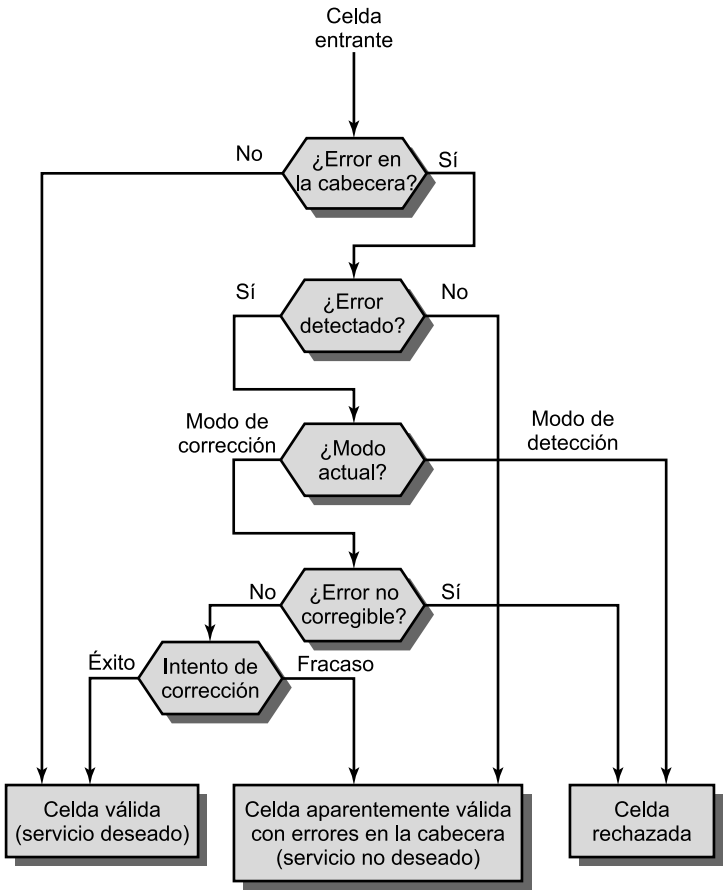


Figura 11.6. Efecto de un error en la cabecera de una celda.

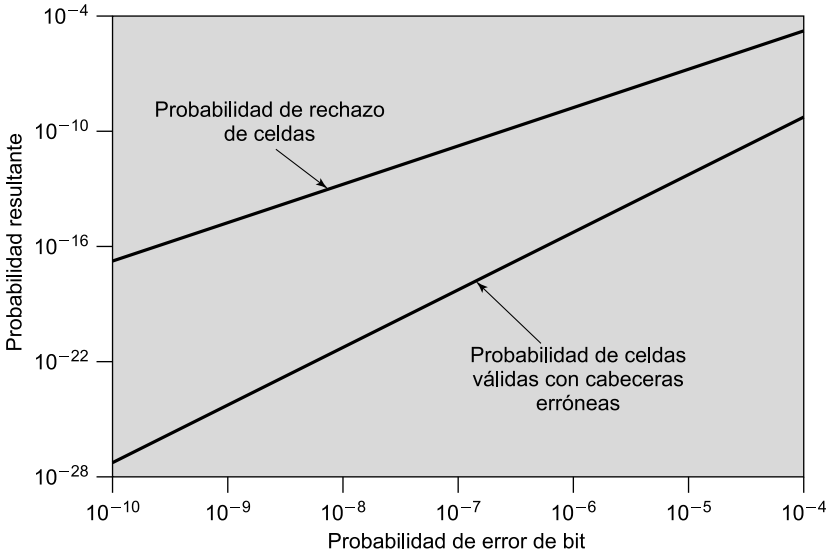


Figura 11.7. Impacto de errores de bit aleatorios en las prestaciones del HEC.

11.4. TRANSMISIÓN DE CELDAS ATM

El documento I.432 especifica que las celdas ATM se pueden transmitir a distintas velocidades: 622,08 Mbps, 155,52 Mbps, 51,84 Mbps o 25,6 Mbps, siendo necesario especificar la estructura de transmisión a usar para el transporte de la carga útil. En el documento referido se definen dos enfoques: una capa física basada en celdas y una capa física basada en SDH[2]. A continuación se estudia cada una de ellas.

CAPA FÍSICA BASADA EN CELDAS

Para la capa física basada en celdas no se impone fragmentación o delimitación, consistiendo la estructura de la interfaz en una secuencia continua de celdas de 53 octetos. Dado que no existe imposición externa de tramas en esta aproximación, es necesaria alguna forma de llevar a cabo la sincronización. Ésta se consigue con el campo de control de errores de cabecera (HEC) incluido en la cabecera de la celda, siendo el procedimiento como sigue (*véase* Figura 11.8):

1. En el estado HUNT se ejecuta un algoritmo de delimitación de celdas bit a bit para determinar el cumplimiento de la regla de codificación HEC (es decir, coincidencia entre el HEC recibido y el calculado). Una vez obtenida una coincidencia, se supone que se ha encontrado una cabecera, pasando el método al estado PRESYNC.
2. En el estado PRESYNC se supone una estructura de celda. El algoritmo de delimitación de celdas se lleva a cabo celda a celda hasta que la regla de codificación se confirme δ veces consecutivas.
3. En el estado SYNC se usa el HEC para la detección y corrección de errores (*véase* Figura 11.5). La delimitación de la celda se supone perdida si la regla de codificación HEC resulta incorrecta α veces consecutivas.

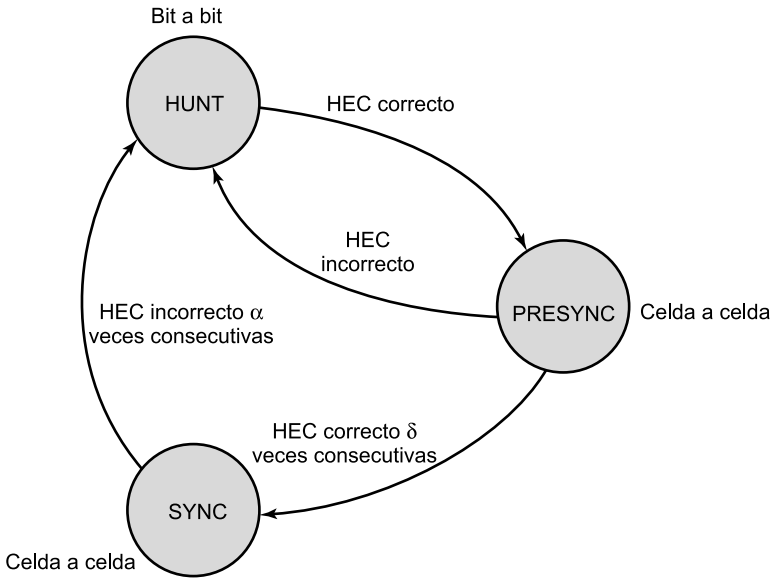


Figura 11.8. Diagrama de estados del procedimiento de delimitación de celdas.

[2] La aproximación basada en SDH no está definida para 25,6 Mbps.

Los valores de α y δ son parámetros de diseño. Valores de δ elevados provocan grandes retardos en la sincronización, pero mayor robustez frente a falsas delimitaciones. Por su parte, valores grandes de α incrementan los retardos en la detección de desalineamientos, aunque también aumentan la robustez frente a falsos desalineamientos. En las Figuras 11.9 y 11.10, basadas en el

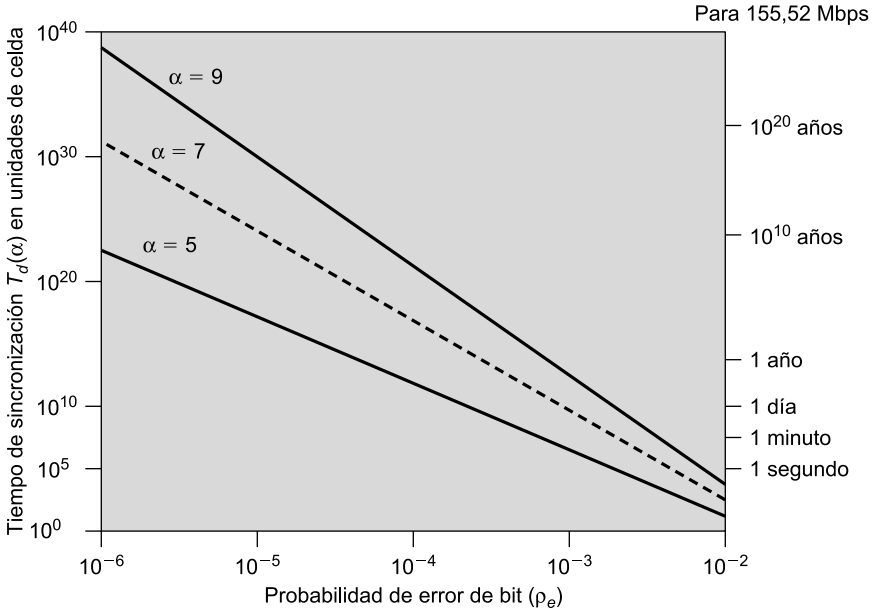


Figura 11.9. Impacto de errores de bit aleatorios en las prestaciones de la delimitación de celdas.

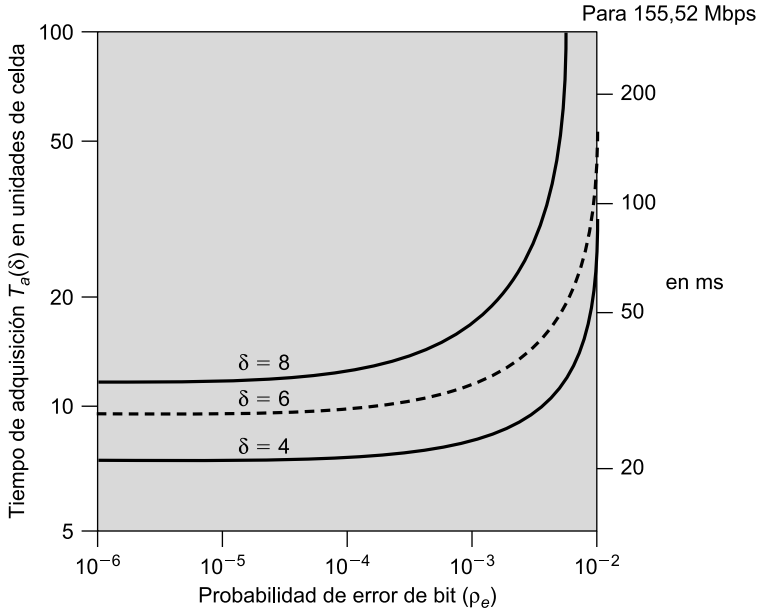


Figura 11.10. Tiempo de adquisición en función de la probabilidad de error de bit.

documento I.432, se muestra el impacto de errores en bits aleatorios sobre las prestaciones de la delimitación de celdas para distintos valores de α y δ. La primera figura muestra el tiempo promedio que el receptor mantendrá la sincronización en función de la tasa de producción de errores, para distintos valores del parámetro α. La segunda figura muestra el tiempo medio necesario para conseguir la sincronización en función de la tasa de error, para distintos valores de δ.

La ventaja de usar el esquema de transmisión basado en celdas es la sencillez de la interfaz que resulta cuando tanto las funciones en modo de transferencia como las de en modo de transmisión se basan en una estructura común.

CAPA FÍSICA BASADA EN SDH

La capa física basada en SDH impone una estructura sobre la secuencia de celdas ATM. En esta sección se verá la especificación I.432 para 155,52 Mbps, usándose estructuras similares para otras velocidades. En la capa física basada en SDH se impone la delimitación o fragmentación haciendo uso de la trama STM-1 (STS-3). En la Figura 11.11 se muestra la porción de carga útil de una trama STM-1 (*véase* Figura 8.11). Esta carga útil puede estar desplazada respecto del principio de la trama, como indica el puntero en los bits suplementarios de sección. Como puede verse, la carga útil consta de 9 octetos suplementarios de camino y el resto, que contiene las celdas ATM. Dado que la capacidad de la carga útil (2.340 octetos) no es un múltiplo entero del tamaño de la celda (53 octetos), ésta puede superar los límites de la carga útil.

El octeto suplementario de camino H4 se utiliza en el extremo emisor para indicar la próxima ocurrencia de una frontera de celda; es decir, el valor del campo H4 especifica el número de octetos hasta la primera frontera de celda que sigue al octeto H4. El rango de posibles valores es de 0 a 52.

Entre las ventajas de la aproximación basada en SDH se encuentran las siguientes:

- Se puede usar para transportar cargas útiles basadas en ATM o en STM (modo de transferencia síncrono), haciendo posible el despliegue inicial de una infraestructura de transmisión de fibra óptica de alta capacidad para un gran número de aplicaciones basadas en conmutación de circuitos y dedicadas, permitiendo así una fácil migración para el soporte de ATM.

Figura 11.11. Carga útil en STM-1 para transmisión de celdas ATM basada en SDH.

- Algunas conexiones específicas pueden ser de conmutación de circuitos usando un canal SDH. Por ejemplo, el tráfico de una conexión de vídeo a velocidad constante puede transmitirse en base a cargas útiles de la señal STM-1, la cual puede ser conmutada por circuitos. Esto puede resultar más eficiente que la conmutación ATM.
- Haciendo uso de las técnicas de multiplexación síncrona SDH se pueden combinar varias secuencias ATM para construir interfaces de velocidad superior a las ofrecidas de forma específica por la capa ATM. Por ejemplo, se pueden combinar cuatro secuencias ATM distintas, cada una a 155 Mbps (STM-1), para dar lugar a una interfaz de 622 Mbps (STM-4). Esta técnica puede ser más efectiva desde el punto de vista del coste que el uso de una única secuencia ATM a 622 Mbps.

11.5. CLASES DE SERVICIOS ATM

Una red ATM se diseña para poder transmitir simultáneamente diferentes tipos de tráfico, entre los que se encuentra la transmisión en tiempo real de voz, vídeo y tráfico TCP a ráfagas. Aunque cada uno de estos flujos de tráfico se gestiona como una secuencia de celdas de 53 octetos a través de un canal virtual, la forma en que se gestiona cada uno de ellos en la red depende de las características del flujo en cuestión y de los requisitos de la aplicación. Por ejemplo, el tráfico de vídeo en tiempo real se debe transmitir con variaciones mínimas de retardo.

En el Capítulo 14 se estudiará la forma en que una red ATM gestiona distintos tipos de tráfico. En esta sección se resumen las clases de servicios ATM, usadas por un sistema final para identificar el tipo de servicio requerido. En el Foro ATM se han definido las siguientes clases de servicios:

- **Servicio en tiempo real**
  - — A velocidad constante (CBR, *Constant Bit Rate*).
  - — A velocidad variable en tiempo real (rt-VBR, *real-time Variable Bit Rate*).
- **Servicio en no tiempo real**
  - — A velocidad variable en no tiempo real (nrt-VBR, *non-real-time Variable Bit Rate*).
  - — A velocidad disponible (ABR, *Available Bit Rate*).
  - — A velocidad no especificada (UBR, *Unspecified Bit Rate*).
  - — A velocidad de tramas garantizada (GFR, *Guaranteed Frame Rate*).

SERVICIOS EN TIEMPO REAL

La distinción más importante entre aplicaciones se refiere al retardo y a la variabilidad de éste, conocida como fluctuación, que puede tolerar la aplicación. Las aplicaciones en tiempo real implican generalmente un flujo de información hacia un usuario que lo reproduce en una fuente. Por ejemplo, un usuario espera que la recepción de un flujo de información de audio o vídeo tenga lugar de forma continua y homogénea. La falta de continuidad u ocurrencia de pérdidas excesivas provoca una disminución importante en la calidad. Las aplicaciones que conllevan una interacción entre usuarios son muy estrictas respecto del retardo, resultando generalmente perjudicial cualquier retardo que supere unas pocas centenas de milisegundos. En consecuencia, en una red ATM son elevadas las demandas de conmutación y envío de datos en tiempo real.

Velocidad constante (CBR)

El servicio CBR es, quizá, el más sencillo de definir. Se usa en aplicaciones que precisan una velocidad constante fija durante toda la conexión y un retardo de transmisión máximo relativamente estable. CBR se usa comúnmente para información de audio y vídeo sin comprimir. Algunos ejemplos de aplicaciones CBR son los siguientes:

- Vídeoconferencia.
- Audio interactivo (por ejemplo, telefonía).
- Distribución de audio/vídeo (por ejemplo, televisión, enseñanza a distancia, servicios de tipo pago-por-visión —*pay-per-view*—).
- Recuperación de audio/vídeo (por ejemplo, vídeo bajo demanda, audioteca).

Velocidad variable en tiempo real (rt-VBR)

La clase rt-VBR está pensada para aplicaciones sensibles al tiempo; es decir, aquellas que presentan fuertes restricciones respecto al retardo y a la variación de éste. La principal diferencia entre aplicaciones apropiadas para rt-VBR y aquellas indicadas para CBR es que en las primeras la transmisión se realiza a una velocidad que varía en el tiempo, o lo que es lo mismo, una fuente rt-VBR se puede caracterizar por su funcionamiento a ráfagas. Por ejemplo, la aproximación estándar para compresión de vídeo produce una secuencia de tramas de imágenes de tamaño variable, por lo que, dado que el vídeo en tiempo real necesita una velocidad de transmisión de tramas uniforme, la velocidad real variará.

El servicio rt-VBR da más flexibilidad a la red que el servicio CBR, ya que ésta puede multiplexar estadísticamente varias conexiones sobre la misma capacidad dedicada y aun así proporcionar el servicio requerido para cada una de ellas.

SERVICIOS EN NO TIEMPO REAL

Los servicios que no son en tiempo real están pensados para aplicaciones que presentan características de tráfico a ráfagas y no tienen fuertes restricciones por lo que respecta al retardo y a la variación del mismo. Consecuentemente, la red presenta una mayor flexibilidad en la gestión de los flujos de tráfico y puede hacer un mayor uso de la multiplexación estadística para aumentar la eficiencia de la red.

Velocidad variable en no tiempo real (nrt-VBR)

Para algunas aplicaciones que no son en tiempo real es posible caracterizar el flujo de tráfico esperado de forma que la red pueda proporcionar una calidad de servicio (QoS, *Quality of Service*) sustancialmente mejorada desde el punto de vista de las pérdidas y el retardo. Estas aplicaciones pueden hacer uso del servicio nrt-VBR, en donde el sistema final especifica una velocidad de pico de celdas, una velocidad de celdas sostenible o promedio y una medida acerca de cómo de agrupadas o en ráfagas pueden estar las celdas. Con esta información, la red puede reservar recursos para ofrecer un retardo relativamente pequeño y una pérdida de celdas mínima.

El servicio nrt-VBR se puede utilizar para transmisiones de datos que presentan requisitos críticos en cuanto a la respuesta en el tiempo. Algunos ejemplos de ello son reserva de vuelos, transacciones bancarias y supervisión de procesos.

Velocidad no especificada (UBR)

En cualquier instante de tiempo, una cierta cantidad de la capacidad de una red ATM se consume en el transporte de tráfico CBR y tráfico VBR de los dos tipos existentes. Una parte adicional de la capacidad se encuentra disponible por una o las dos razones siguientes: (1) no todos los recursos se han destinado a tráfico CBR y VBR y (2) la naturaleza a ráfagas del tráfico VBR implica que a veces se usa menos capacidad de la reservada. Toda esta capacidad sin usar se encuentra disponible para el servicio UBR, el cual es apropiado para aplicaciones que toleran retardos variables y cierta tasa de pérdida de celdas, lo que resulta generalmente cierto para tráfico TCP. En el servicio UBR, las celdas se transmiten según una cola FIFO (*First-In-First-Out*) haciendo uso de la capacidad no consumida por otros servicios, siendo posible la aparición de retardos y pérdidas variables. Hemos de señalar que en el servicio UBR no se hacen reservas iniciales ni se proporciona realimentación relativa a la congestión, por lo que se conoce como **servicio de mejor esfuerzo**. Algunos ejemplos de aplicaciones UBR son los siguientes:

- Transferencia, mensajería, distribución y recuperación de texto/datos/imágenes.
- Terminal remoto (por ejemplo, teleconmutación).

Velocidad disponible (ABR)

Como se estudiará en el Capítulo 17, las aplicaciones de transmisión a ráfagas que usan un protocolo fiable extremo a extremo como TCP pueden detectar congestión en una red a través del incremento en los retardos de ida y vuelta y en base al rechazo de paquetes. Sin embargo, TCP no dispone de ningún mecanismo para compartir los recursos internos a la red entre varias conexiones; además, TCP no minimiza la congestión tan eficientemente como es posible mediante el uso de información explícita de los nodos de la red congestionados.

Para mejorar el servicio ofrecido a las fuentes de naturaleza a ráfagas, que deberían hacer uso del servicio UBR, se ha definido el servicio ABR. Una aplicación que haga uso de ABR especifica una velocidad de pico de celdas (PCR, *Peak Cell Rate*) a usar y una velocidad de celdas mínima (MCR, *Minimum Cell Rate*) necesaria. La red reserva los recursos de forma que todas las aplicaciones ABR reciban al menos la capacidad MCR indicada, compartiéndose la capacidad no usada de forma equitativa y controlada entre todas las fuentes ABR. El mecanismo ABR hace uso explícito de realimentación hacia las fuentes para asegurar que la capacidad se ha reservado adecuadamente. La capacidad no usada por las fuentes ABR permanece disponible para tráfico UBR.

Un ejemplo de aplicación que usa ABR es la interconexión de redes LAN. En este caso, los sistemas finales conectados a la red ATM son dispositivos de encaminamiento.

En la Figura 11.12 se sugiere cómo una red lleva a cabo la reserva de recursos durante un periodo de tiempo estable (no se añaden ni se eliminan canales virtuales).

Velocidad de tramas garantizada (GFR)

El servicio GFR es el de más reciente adopción en ATM y está diseñado específicamente para dar servicio a subredes troncales IP. GFR proporciona mejor servicio que UBR para tráfico basado en tramas, incluyendo el tráfico de tipo IP y Ethernet. El principal objetivo de GFR es la optimización de la gestión del tráfico basado en tramas que va desde una LAN a una red troncal ATM a través de un dispositivo de encaminamiento. El tipo de redes ATM mencionado está siendo usado de forma creciente en redes de grandes empresas, de operadores y de proveedores de servicios de Internet con objeto de consolidar y extender los servicios IP sobre redes de área amplia. Aunque ABR

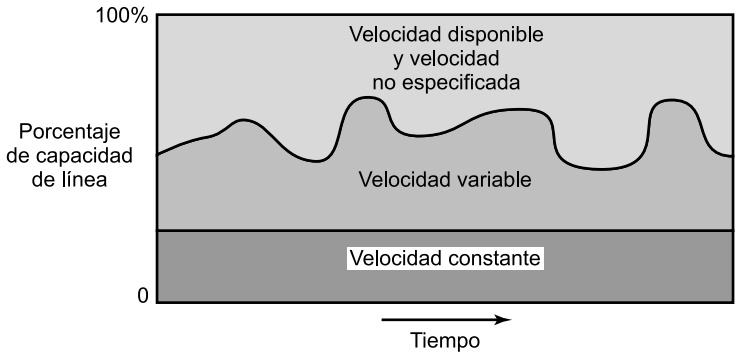


Figura 11.12. Servicios ATM a distintas velocidades.

es también un servicio pensado para mejorar la transmisión de paquetes sobre redes ATM, resulta relativamente difícil de implementar entre dispositivos de encaminamiento en una red ATM. Debido al aumento en el uso de ATM para dar soporte a tráfico IP, en especial el originado en LAN de tipo Ethernet, GFR puede resultar una alternativa más atractiva que ABR para proporcionar un servicio ATM.

Una de las técnicas empleadas por GFR para proporcionar mejores prestaciones que UBR consiste en hacer que los elementos de la red conozcan las fronteras de las tramas o paquetes. De este modo, cuando la ocurrencia de congestión precisa el rechazo de celdas, los elementos de la red deben rechazar todas aquellas que componen una sola trama. GFR también permite a un usuario llevar a cabo la reserva de capacidad para cada VC GFR, garantizándose la capacidad mínima indicada y pudiendo transmitirse tramas adicionales si la red no se encuentra congestionada.

11.6. CAPA DE ADAPTACIÓN ATM

El uso de ATM hace necesaria la existencia de una capa de adaptación para dar soporte a protocolos de transferencia de información que no estén basados en ATM. Dos ejemplos de ello son voz PCM (modulación por código de pulso) y el protocolo Internet (IP). Voz PCM es una aplicación que genera una secuencia de bits a partir de una señal de voz. Para utilizar esta aplicación sobre ATM es necesario agrupar bits PCM en celdas para su transmisión y leerlas cuando sean recibidas en el receptor de manera que se obtenga un flujo homogéneo y constante de bits. En un entorno heterogéneo en el que existen redes IP interconectadas con redes ATM, una forma adecuada de integrar los dos tipos de redes es realizar una transformación entre paquetes IP y celdas ATM; esto implicará en general la segmentación de un paquete IP en varias celdas para su transmisión y el ensamblado de la trama a partir de las celdas en el receptor. Permitiendo el uso de IP sobre ATM es posible la utilización de toda la infraestructura IP existente sobre una red ATM.

SERVICIOS AAL

El documento I.362 de ITU-T especifica los siguientes ejemplos generales de servicios ofrecidos por AAL:

- Gestión de errores de transmisión.
- Segmentación y ensamblado para permitir la transmisión de bloques de datos mayores en el campo de información de las celdas ATM.

- Gestión de condiciones de pérdida de celdas y de celdas mal insertadas.
- Control de flujo y de temporización.

Con objeto de minimizar el número de protocolos AAL diferentes que se deben especificar para dar respuesta a las distintas necesidades, ITU-T ha definido cuatro clases de servicios que cubren un amplio rango de requisitos. La clasificación se realiza teniendo en cuenta si se debe mantener una relación de temporización entre el emisor y el receptor, si la aplicación necesita una velocidad constante y si la transferencia es o no orientada a conexión. El sistema de clasificación no se encuentra en ningún documento de la ITU-T, pero el concepto ha permitido el desarrollo de los protocolos AAL. Esencialmente, la capa AAL proporciona mecanismos para dar soporte a una amplia variedad de aplicaciones sobre la capa ATM y ofrece protocolos construidos sobre la base de las capacidades de gestión de tráfico de la capa ATM. En consecuencia, el diseño de los protocolos AAL debe estar relacionado con las clases de servicio estudiadas en la Sección 11.5.

En la Tabla 11.4, basada en una tabla de [MCDY99], se relacionan los cuatro protocolos AAL para las clases de servicios definidas por el Foro ATM. En dicha tabla se sugieren los tipos de aplicaciones que pueden soportar conjuntamente AAL y ATM. Entre ellas se encuentran las siguientes:

Tabla 11.4. Protocolos y servicios AAL.

	CBR	rt-VBR	nrt-VBR	ABR	UBR
AAL 1	Emulación de circuitos, RDSI, voz sobre ATM				
AAL 2		Voz y vídeo VBR			
AAL 3/4			Servicios generales de datos		
AAL 5	Emulación de redes LAN	Voz bajo demanda, emulación LANE	Retransmisión de tramas, ATM, emulación LANE	Emulación LANE	IP sobre ATM

- **Emulación de circuitos:** hace referencia al soporte de estructuras de transmisión TDM síncronas como T-1, sobre redes ATM.
- **Voz y vídeo VBR:** son aplicaciones en tiempo real que se transmiten en formato comprimido. Un efecto de la compresión es que la aplicación puede estar soportada por una velocidad variable, lo que requiere un envío continuo de bits hacia el destino.
- **Servicios generales de datos:** entre ellos se incluyen servicios de mensajería y transacciones que no precisan soporte en tiempo real.
- **IP sobre ATM:** transmisión de paquetes IP en celdas ATM.
- **Encapsulado multiprotocolo sobre ATM (MPOA):** soporte de protocolos distintos de IP (por ejemplo, IPX, AppleTalk, DECNET) sobre ATM.
- **Emulación de redes LAN (LANE):** soporte de tráfico entre redes LAN a través de redes ATM, con emulación de la capacidad de difusión LAN (la transmisión de una estación se recibe en muchas otras estaciones). LANE se diseña para permitir una transición cómoda entre un entorno LAN y uno ATM.

PROTOCOLOS AAL

La capa AAL se organiza en dos subcapas lógicas: la de convergencia (CS, *Convergence Sublayer*) y la de segmentación y agrupación o ensamblado (SAR, *Segmentation And Reassembly sublayer*). La primera proporciona las funciones necesarias para dar soporte a aplicaciones específicas que hacen uso de AAL. Cada usuario AAL se conecta a la capa AAL a través de un punto de acceso al servicio (SAP, *Service Access Point*), que no es más que la dirección de la aplicación. Esta subcapa es, por tanto, dependiente del servicio.

La subcapa de segmentación y ensamblado es responsable de empaquetar la información recibida desde la subcapa CS en celdas para su transmisión y desempaquetar la información en el otro extremo. Como ya hemos visto, cada celda en la capa ATM consta de una cabecera de 5 octetos y de un campo de información de 48 octetos; por tanto, la subcapa SAR debe empaquetar las cabeceras y colas SAR y añadir información de la subcapa CS en bloques de 48 octetos.

En la Figura 11.13 se indica la arquitectura de protocolos general para ATM y AAL. Normalmente, un bloque de datos procedente de una capa superior se encapsula en una unidad de datos de protocolo (PDU, *Protocol Data Unit*), consistente en los datos de la capa superior y, posiblemente, una cabecera y una cola con información de protocolo del nivel CS. Esta PDU de la subcapa CS se pasa después hacia abajo a la capa SAR y se segmenta en varios bloques, cada uno de los cuales se encapsula en una PDU SAR de 48 octetos que puede incluir una cabecera y una cola además del bloque de datos procedente de la subcapa CS. Por último, cada PDU SAR constituye el campo de carga útil de una sola celda ATM.

Inicialmente, ITU-T definió cuatro tipos de protocolos, llamados Tipo 1 a Tipo 4. Realmente, cada tipo de protocolo consta de dos protocolos, uno en la subcapa CS y otro en la subcapa SAR. Recientemente se han unido los tipos 3 y 4, dando lugar al protocolo Tipo 3/4, y se ha definido un nuevo tipo, el Tipo 5. En todos los casos, un bloque de datos procedente de una capa superior se encapsula en una unidad de datos de protocolo (PDU) de la subcapa CS. De hecho, esta subcapa se

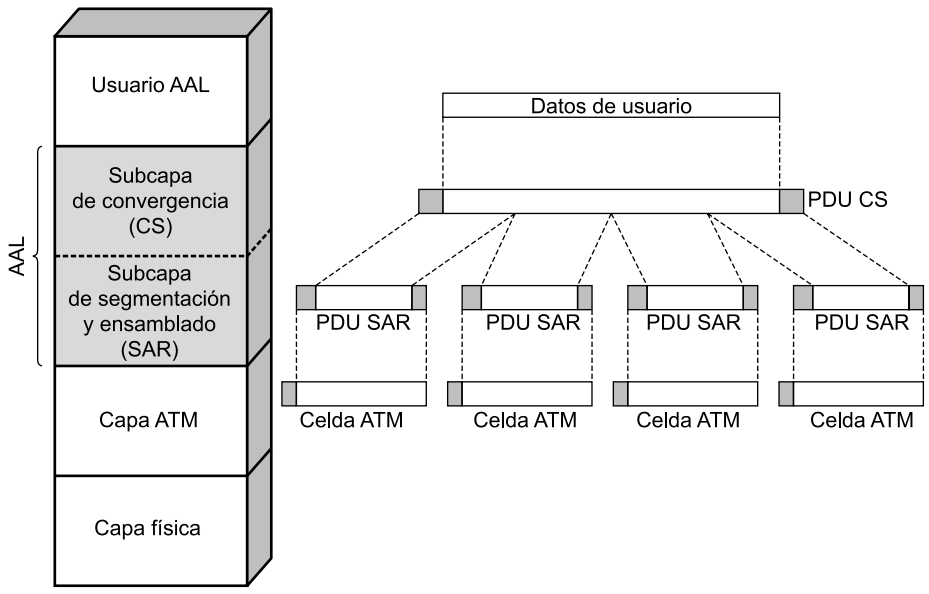


Figura 11.13. Protocolos y PDU AAL.

conoce subcapa de convergencia común (CPCS, *Common Part Convergence Sublayer*), dejando abierta la posibilidad de que se puedan realizar funciones adicionales especializadas en la subcapa CS. La PDU CPCS se pasa posteriormente a la subcapa SAR, donde se trocea en bloques de carga útil. Cada uno de estos bloques se puede incluir en una PDU de la subcapa SAR, la cual tiene una longitud total de 48 octetos. A su vez, cada PDU SAR de 48 octetos se encapsula en una sola celda ATM.

En la Figura 11.14 se muestran los formatos de las unidades de datos de protocolo (PDU) correspondientes a los tipos 1 y 5.

AAL Tipo 1

En la operación de Tipo 1 se trabaja con fuentes de velocidad constante, siendo la única responsabilidad del protocolo SAR la de empaquetar los bits en celdas para su transmisión y desempaquetarlos en el extremo receptor. Cada bloque se acompaña de un **número de secuencia** (SN) de forma que se pueda seguir la pista de las PDU erróneas. El campo SN, de 4 bits, consiste en un bit indicador de la subcapa de convergencia (CSI) y un contador de secuencia (SC) de 3 bits. En el proceso de transmisión, la subcapa CS proporciona un valor CSI a la subcapa SAR para su inclusión en el campo SN, pasando la subcapa SAR este valor hacia la subcapa CS en el proceso de recepción. El bit CSI se emplea para transmitir información de la siguiente forma. El contador de secuencia de 3 bits define una estructura de trama consistente en 8 celdas ATM consecutivas, numeradas del 0 al 7. Los valores del bit CSI en las celdas 1, 3, 5 y 7 se interpretan como un valor de tiempo de 4 bits, usado para proporcionar una medida de la diferencia de frecuencia entre el reloj de referencia de la red y el del emisor. Por su parte, en las celdas pares, el bit CSI se puede usar para realizar el empaquetado de la información procedente de una capa superior: si este bit vale uno en una celda par (0, 2, 4, 6), el primer octeto del campo de carga útil de la PDU SAR es un puntero que indica el comienzo del siguiente bloque estructurado dentro de la carga útil de ésta y de la siguiente celda; es decir, dos celdas (0-1, 2-3, 4-5, 6-7) se tratan como si contuviesen un puntero de un octeto y una carga útil de 93 octetos, indicando el puntero cuál es el primer octeto del siguiente bloque de datos dentro de la carga útil de 93 octetos. El valor de desplazamiento 93 se utiliza para indicar que el final de la carga útil de 93 octetos coincide con el final de un bloque estructurado, usándose el valor 127 cuando no se indica frontera de estructura alguna.

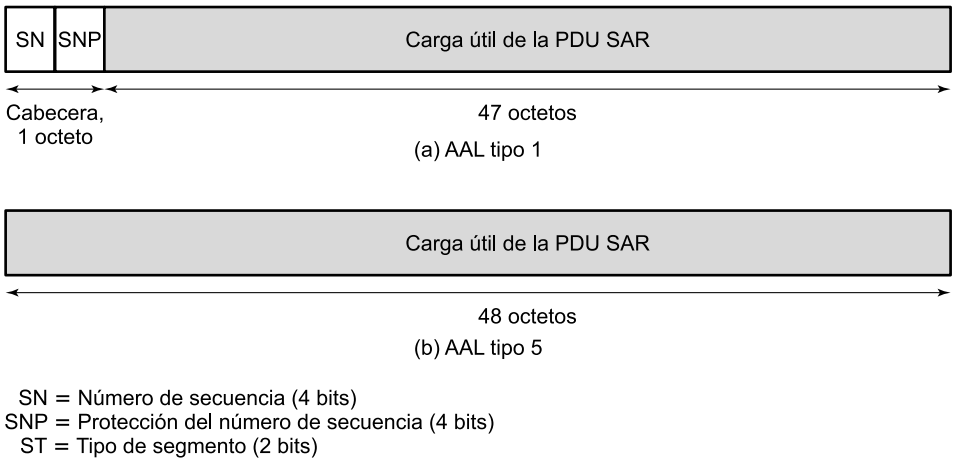

SN
SNP
Carga útil de la PDU SAR
Cabecera,
1 octeto
47 octetos
(a) AAL tipo 1
Carga útil de la PDU SAR
48 octetos
(b) AAL tipo 5
SN = Número de secuencia (4 bits)
SNP = Protección del número de secuencia (4 bits)
ST = Tipo de segmento (2 bits)

Figura 11.14. Unidades de datos de protocolo (PDU) de segmentación y ensamblado (SAR).

Como se ha visto, el campo SC de 3 bits proporciona una estructura de trama de 8 celdas, al tiempo que una forma de llevar a cabo la detección de celdas perdidas/desordenadas.

El campo de **protección del número de secuencia** (SNP) es un código de error para la detección y posible corrección de errores sobre el campo de número de secuencia. El campo SNP consta de una secuencia de comprobación de redundancia cíclica (CRC) de 3 bits, calculada sobre el campo SN de 4 bits, y de un bit de paridad, el cual se fija de modo que la paridad de la cabecera SAR de 8 bits sea par.

No se ha definido PDU CS alguna para el Tipo 1, estando en este caso relacionadas las funciones de la subcapa CS con la temporización y la sincronización y no siendo necesaria una cabecera CS independiente.

AAL Tipo 2 y Tipo 3/4

El resto de los tipos de protocolo (2, 3/4 y 5) gestionan información de velocidad variable. El Tipo 2 está destinado a aplicaciones analógicas, como vídeo y audio, que necesitan información temporal pero no precisan una velocidad constante. Se ha retirado una especificación inicial dada para los protocolos de Tipo 2 (SAR y CS), enunciándose en la versión actual del documento I.363 una simple lista de servicios y funciones a proveer.

Las especificaciones iniciales de la capa AAL de Tipo 3 y de Tipo 4 eran muy similares en cuanto al formato de la PDU y a la funcionalidad. Consecuentemente, ITU-T decidió combinar los dos tipos en una sola especificación de protocolo para las subcapas SAR y CS, conocida como Tipo 3/4.

Los tipos de servicio proporcionados por AAL Tipo 3/4 se pueden caracterizar de acuerdo a dos consideraciones:

1. El servicio puede ser orientado o no a conexión. En el segundo caso, cada bloque de datos pasado a la capa SAR (unidad de datos de servicio de SAR o SDU SAR) se trata de forma independiente, mientras que en el caso del servicio orientado a conexión es posible definir varias conexiones lógicas SAR sobre una misma conexión ATM.
2. El servicio puede realizarse en modo de mensaje o en modo continuo. En el primer tipo de servicio se transfieren los datos por medio de tramas, teniendo así cabida en dicho tipo de servicio los protocolos y aplicaciones OSI; en particular, LAPD o la técnica de retransmisión de tramas (*frame relay*) se podrían llevar a cabo en modo de mensaje: un único bloque de datos de la capa superior a AAL se transmite en una o más celdas. Por su parte, el servicio en modo continuo implica la transferencia continua de datos de baja velocidad con requisitos de bajo retardo; en este caso, los datos se pasan a AAL en bloques de tamaño fijo que pueden ser tan pequeños como un octeto, transmitiéndose un bloque por celda.

El protocolo AAL de Tipo 3/4 lleva a cabo su servicio de transferencia de datos aceptando bloques de éstos de la capa inmediatamente superior y transmitiendo cada uno de ellos hacia el usuario AAL de destino. Dado que la capa ATM limita la transferencia de datos a la carga útil de 48 octetos de una celda, la capa AAL debe realizar, como mínimo, una función de segmentación y ensamblado.

La aproximación considerada en AAL Tipo 3/4 es la que sigue. Un bloque de datos de una capa superior, como una PDU, se encapsula en una PDU de la subcapa CPCS, la cual se pasa a la subcapa SAR y se segmenta en bloques de carga útil de 44 octetos. Cada bloque de carga útil se

encapsula en una PDU SAR, que incluye una cabecera y una cola en un total de 48 octetos de longitud. Finalmente, cada PDU SAR de 48 octetos se encapsula en una sola celda ATM.

Una característica distintiva de AAL Tipo 3/4 es que puede multiplexar varias secuencias de datos sobre la misma conexión ATM virtual (VCI/VPI). En el servicio orientado a conexión, a cada conexión lógica entre usuarios AAL se le asigna un valor MID único de 10 bits, de modo que se puede multiplexar y mezclar sobre una sola conexión ATM el tráfico de celdas procedente de hasta 2^{10} conexiones AAL distintas. En el caso del servicio no orientado a conexión, el campo MID se puede usar para comunicar un identificador único asociado a cada usuario del servicio y, de nuevo, se puede multiplexar el tráfico procedente de varios usuarios AAL.

AAL Tipo 5

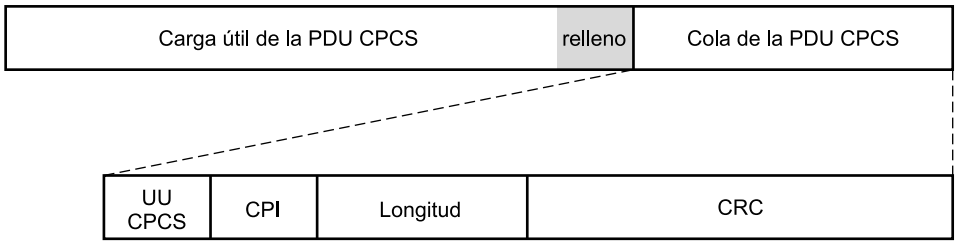
AAL 5 se introdujo para proporcionar un servicio de transporte funcional para protocolos de capa superior orientados a conexión. Si se supone que la capa superior lleva a cabo la gestión de la conexión y que la capa ATM produce errores mínimos, no son necesarios la mayor parte de los campos de las PDU SAR y CPCS de Tipo 3/4. Por ejemplo, el campo MID no es necesario para el servicio orientado a conexión: el VCI/VPI se encuentra disponible para la multiplexación celda a celda y la capa superior admite multiplexación mensaje a mensaje.

El Tipo 5 se introdujo para:

- Reducir el coste suplementario de procesamiento del protocolo.
- Reducir el coste de la transmisión.
- Asegurar la adaptabilidad a los protocolos de transporte existentes.

En las Figuras 11.14b y 11.15 se muestran los formatos de las PDU de las subcapas SAR y CPCS para el Tipo 5. Para comprender el funcionamiento del Tipo 5, comencemos por la capa CPCS. La PDU de esta capa incluye una cola con los siguientes campos:

- **Indicador usuario-usuario CPCS (1 octeto):** usado para la transferencia transparente de información entre usuarios.
- **Indicador de parte común (1 octeto):** indica la interpretación del resto de campos de la cola de la PDU CPCS. Actualmente sólo se encuentra definida una interpretación.



UU CPCS = Indicador usuario-usuario CPCS (1 octeto)
CPI = Indicador de parte común (1 octeto)
Longitud = Longitud de la carga útil de la PDU CPCS (2 octetos)
CRC = Comprobación de redundancia cíclica (4 octetos)

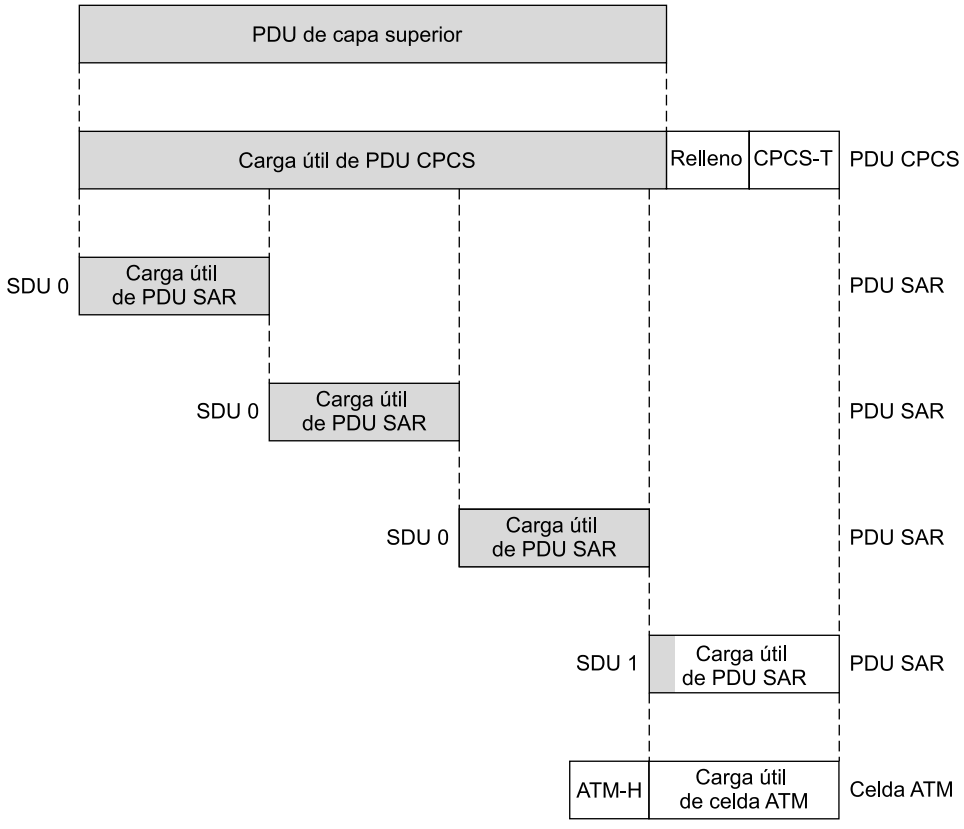
Figura 11.15. PDU AAL 5.

- **Longitud (2 octetos):** longitud del campo de carga útil de la PDU CPCS.
- **Comprobación de redundancia cíclica (4 octetos):** campo empleado para detectar errores de bits en la PDU CPCS.

Una secuencia CRC de 32 bits protege la PDU CPCS entera, mientras que en el caso de AAL de Tipo 3/4 se usa un CRC de 10 bits en cada PDU SAR. El campo CRC usado en el protocolo AAL Tipo 5 proporciona una fuerte protección contra errores de bits al tiempo que, como se muestra en [WANG92], una detección robusta de celdas desordenadas, situación que podría darse ante ciertas condiciones de mal funcionamiento de la red.

La carga útil de la capa superior se somete a un relleno de modo que el tamaño total de la PDU CPCS sea múltiplo de 48 octetos. Así, parte de la PDU CPCS se transportará en el campo de carga útil de la PDU SAR, de sólo 48 octetos de longitud. La ausencia de coste suplementario del protocolo tiene varias implicaciones:

- Dado que no existe número de secuencia, el receptor debe suponer que todas las PDU de la capa SAR llegan en el orden adecuado para su ensamblado, utilizándose el campo CRC de la PDU CPCS para verificar este hecho.



CPCS = Subcapa de convergencia común
SAR = Segmentación y ensamblado
PDU = Unidad de datos de protocolo
CPCS-T = Cola de CPCS
ATM-H = Cabecera ATM
SDU = Bit indicador del tipo de unidad de datos de servicio

Figura 11.16. Ejemplo de transmisión AAL 5.

- La ausencia del campo MID implica que no es posible la mezcla de celdas correspondientes a diferentes PDU de la subcapa CPCS. Por tanto, cada PDU SAR sucesiva contiene una parte de la PDU CPCS actual o el primer bloque de la PDU CPCS siguiente. Para distinguir entre estos dos casos se usa el bit indicador de tipo de la SDU ATM en el campo de tipo de carga útil de la cabecera de la celda ATM (*véase* Figura 11.4). Una PDU CPCS consiste en cero o más PDU SAR consecutivas con el bit tipo de SDU igual a 0, seguidas inmediatamente por una PDU SAR con el bit mencionado puesto a 1.

- La no existencia del campo LI significa que no hay forma de que la entidad SAR distinga entre octetos correspondientes a una PDU CPCS y bits de relleno en el caso de la última PDU SAR. Así pues, no hay manera de que la entidad SAR encuentre la cola de la PDU CPCS en la última PDU SAR. Para evitar este hecho, se precisa que la carga útil de la PDU CPCS se rellene de forma que el último bit de la cola CPCS coincida con el último bit de la PDU SAR final.

En la Figura 11.16 se muestra un ejemplo de transmisión AAL 5. La PDU CPCS, incluyendo los datos de relleno y la cola, se divide en bloques de 48 octetos, cada uno de los cuales se transmite en una sola celda ATM.

11.7. LECTURAS Y SITIOS WEB RECOMENDADOS

[MCDY99] y [BLAC99] presentan un estudio en profundidad de ATM. Por su parte, la aproximación de camino virtual/canal virtual en ATM se examina en [SATO90], [SATO91] y [BURG91].

[GARR96] presenta las clases de servicios ATM y discute las implicaciones sobre la gestión de tráfico de cada uno de ellos. [ARMI93] y [SUZU94] discuten AAL y comparan los tipos 3/4 y 5.

ARMI93 Armitage, G., y Adams, K. «Packet Reassembly During Cell Loss.» *IEEE Network*, septiembre 1995.

BLAC99 Black, U. *ATM Volume I*: *Foundation for Broadband Networks*. Upper Saddle River, NJ: Prentice Hall, 1992.

BURG91 Burg, J. y Dorman, D. «Broadband ISDN Resource Management: The Role of Virtual Paths.» *IEEE Communications Magazine*, septiembre 1991.

GARR96 Garrett, M. «A Service Architecture for ATM: From Applications to Scheduling.» *IEEE Network*, mayo/junio 1996.

MCDY99 McDysan, D., y Spohn, D. *ATM: Theory and Application.* New York: McGraw-Hill, 1999.

SATO90 Sato, K.; Ohta, S.; y Tokizawa, I. «Broad-band ATM Network Architecture Based on Virtual Paths.» *IEEE Transactions on Communications*, agosto 1990.

SATO91 Sato, K.; Ueda, H.; y Yoshikai, M. «The Role of Virtual Path Crossconnection.» *IEEE LTS*, agosto 1991.

SUZU94 Suzuki, T. «ATM Adaptation Layer Protocol.» *IEEE Communications Magazine*, abril 1995.

SITIOS WEB RECOMENDADOS

- **Enlaces de interés sobre ATM:** conjunto de informes oficiales y enlaces mantenidos por la Universidad de Minnesota.
- **Foro ATM:** contiene especificaciones técnicas, documentos oficiales y copias actualizadas de la publicación 53 *Bytes* del Foro.
- **Refugio de la retransmisión de celdas:** contiene archivos de listas de correo de la retransmisión de celdas y enlaces a numerosos documentos y sitios web relacionados con ATM.

11.8. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

camino virtual
canal virtual
capa de adaptación ATM (AAL)
control de errores de cabecera (HEC)
control de flujo genérico (GFR)
modo de transferencia asíncrono (ATM)
prioridad de pérdida de celdas (CLP)
tipo de carga útil
unidad de datos de servicio (SDU)
velocidad constante (CBR)
velocidad de tramas garantizada (GFR)
velocidad disponible (ABR)
velocidad no especificada (UBR)
velocidad variable (VBR)
velocidad variable en no tiempo real (nrt-VBR)
velocidad variable en tiempo real (rt-VBR)

CUESTIONES DE REPASO

11.1. ¿En qué se diferencia ATM de la técnica de retransmisión de tramas (*frame relay*)?

11.2. ¿Cuáles son las ventajas y desventajas de ATM frente a técnica de retransmisión de tramas (*frame relay*)?

11.3. ¿Qué diferencia existe entre un canal virtual y un camino virtual?

11.4. ¿Cuáles son las ventajas de usar caminos virtuales?

11.5. ¿Cuáles son las características de una conexión de canal virtual?

11.6. ¿Cuáles son las características de una conexión de camino virtual?

11.7. Enuncie y explique brevemente los campos de las celdas ATM.

11.8. Explique de forma breve dos métodos para la transmisión de celdas ATM.

11.9. Enuncie y defina brevemente las clases de servicios ATM.

11.10. ¿Qué servicios proporciona AAL?

EJERCICIOS

11.1. Liste los 16 posibles valores del campo GFC y la interpretación de cada uno de ellos (algunos valores no son válidos).

11.2. Una decisión de diseño importante en ATM es el uso de celdas de tamaño fijo o variable. Consideremos esta decisión desde el punto de vista de la eficiencia. La eficiencia de la transmisión se puede definir como:

$$N = \frac{\text{número de octetos de información}}{\text{número de octetos de información} + \text{número de octectos suplementarios}}$$

a) En el caso de paquetes de longitud fija, la información suplementaria consiste en los octetos de cabecera. Definamos:

L = tamaño del campo de datos de la celda, en octetos.

H = tamaño de la cabecera de la celda, en octetos.

X = número de octetos de información a transmitir como un único mensaje.

Obtenga una expresión para N. *Sugerencia:* la expresión requiere el uso del operador $\lceil \cdot \rceil$, donde $\lceil Y \rceil$ = menor entero mayor o igual que Y.

b) Si las celdas son de longitud variable, los octetos suplementarios se determinan como la cabecera más los indicadores para delimitar las celdas o un campo de longitud adicional en la cabecera. Sea H_v el número de octetos suplementarios adicionales necesarios para posibilitar el uso de celdas de longitud variable. Obtenga una expresión para N en función de X, H y H_v.

c) Sea $L = 48$, $H = 5$ y $H_v = 2$. Dibuje N en función del tamaño del mensaje para celdas de tamaño fijo y variable. Comente los resultados.

11.3. Otra decisión de diseño importante en ATM es el tamaño del campo de datos para celdas de longitud fija. Consideremos esta decisión desde el punto de vista de la eficiencia y del retardo.

a) Suponga que tiene lugar una transmisión larga, de modo que todas las celdas están completamente llenas. Obtenga una expresión para la eficiencia N en función de H y L.

b) El retardo de empaquetamiento es el retardo introducido en la transmisión de una secuencia ante la necesidad de almacenar temporalmente los bits hasta que se haya completado un paquete para su transmisión. Obtenga una expresión para este retardo en función de L y de la velocidad R de la fuente.

c) Velocidades de transmisión usuales para codificación de voz son 32 kbps y 64 kbps. Represente el retardo de empaquetamiento en función de L para estas dos velocidades; use un eje y izquierdo con valor máximo de 2 ms. Dibuje en la misma gráfica la eficiencia de la transmisión en función de L; use un eje y derecho con un valor máximo del 100%. Comente los resultados.

11.4. Suponga la transmisión de vídeo comprimido en una red ATM en la que las celdas ATM estándares se transmiten a través de 5 conmutadores y la velocidad de datos es 43 Mbps.

a) ¿Cuál es el tiempo de transmisión de una celda sobre un conmutador?

b) Los conmutadores pueden transmitir celdas correspondientes a tráfico de prioridad inferior, de modo que si un conmutador dado está ocupado transmitiendo una celda, una nueva celda recibida debe esperar hasta que se complete la anterior. En cambio, si el conmutador está libre, la celda recibida se transmitirá inmediatamente. ¿Cuál es el tiempo máximo transcurrido desde que una celda de vídeo se recibe en el primer

conmutador (y posiblemente espera) hasta que es transmitida por el quinto y último? Suponga despreciables el tiempo de propagación, el de conmutación y cualquier otro salvo el tiempo de transmisión y el de espera hasta que se transmiten celdas previas.

c) Suponga ahora que los conmutadores dedican el 60% del tiempo a tráfico de prioridad baja; es decir, la probabilidad de encontrar ocupado un conmutador es 0,6. Suponga también que si un conmutador está transmitiendo una celda, el retardo medio de espera para la finalización de dicha transmisión es la mitad del tiempo de transmisión de la celda. ¿Cuál es el tiempo medio transcurrido desde la entrada al primer conmutador hasta la salida por el quinto?

d) Sin embargo, la medida más interesante no es el retardo, sino la variabilidad de éste (*jitter*). Calcule la variabilidad máxima y media del retardo a partir de los apartados (b) y (c), respectivamente.

Suponga en todos los casos que los diferentes sucesos aleatorios son independientes entre sí. Por ejemplo, ignore la naturaleza a ráfagas típica de dicho tráfico.

11.5. Suponga que se usa AAL 3/4 y que el receptor se encuentra en un estado desocupado (no se reciben celdas). A continuación, se transmite un bloque de datos de usuario como una secuencia de PDU SAR.

a) Suponiendo que la PDU SAR BOM se pierde, ¿qué sucede en el receptor?

b) ¿Qué ocurrirá en el extremo receptor si se pierde una de las PDU SAR COM?

c) Supongamos que se pierden 16 PDU SAR COM consecutivas. ¿Qué sucede en el receptor?

d) ¿Qué ocurrirá en el extremo receptor si se perdiese de forma consecutiva un número múltiplo de 16 PDU SAR COM?

11.6. Haciendo uso de nuevo de AAL 3/4, suponga que el receptor se encuentra en un estado desocupado y que se transmiten dos bloques de datos de usuario como dos secuencias diferentes de PDU SAR.

a) Suponga que se pierde la PDU SAR EOM de la primera secuencia. ¿Qué ocurrirá en el extremo receptor?

b) Supóngase ahora que se pierde la PDU SAR EOM de la primera secuencia y la PDU SAR BOM de la segunda. ¿Qué sucederá en el receptor?

11.7. Supongamos que se utiliza AAL 5 y que el extremo receptor se encuentra en un estado desocupado (no se reciben celdas). Transmitido un bloque de datos de usuario como una secuencia de PDU SAR:

a) ¿Qué ocurriría en el extremo receptor si se produjese un error simple en una de las PDU SAR?

b) Suponga ahora que se pierde una de las celdas con el bit de tipo de SDU igual a 0. ¿Qué sucederá en el receptor?

c) ¿Qué ocurrirá en el extremo receptor si se supone que se pierde una de las celdas con el bit de tipo de SDU igual a 1?

CAPÍTULO 12

Encaminamiento en redes conmutadas

12.1. Encaminamiento en redes de conmutación de circuitos

12.2. Encaminamiento en redes de conmutación de paquetes
Características
Estrategias de encaminamiento
Ejemplos

12.3. Algoritmos de mínimo coste
Algoritmo de Dijkstra
Algoritmo de Bellman-Ford
Comparación

12.4. Lecturas recomendadas

12.5. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- El encaminamiento en redes de conmutación de circuitos se ha basado tradicionalmente en esquemas estáticos, donde se consideran rutas alternativas para dar respuesta a aumentos de carga. Los esquemas de encaminamiento actuales proporcionan estrategias más adaptables y flexibles.
- La función de encaminamiento de una red de conmutación de paquetes trata de encontrar la ruta de mínimo coste a través de la red, estando el parámetro de coste basado en el número de saltos, el retardo esperado u otras métricas. Los algoritmos de encaminamiento adaptables se fundamentan generalmente en el intercambio de información relativa a las condiciones de tráfico entre los nodos.

Un aspecto clave de diseño de las redes conmutadas, entre las que se encuentran las de conmutación de paquetes, de retransmisión de tramas, las redes ATM y las redes internet, es el relativo al encaminamiento. En términos generales, esta función trata de encontrar rutas a través de la red entre pares de nodos finales comunicantes, de modo que la red se use de forma eficiente.

Este capítulo comienza con un breve estudio de los aspectos involucrados en el encaminamiento en redes de conmutación de circuitos. Seguidamente, se verá el encaminamiento en redes de conmutación de paquetes y se examinarán los algoritmos de mínimo coste, parte fundamental en el encaminamiento en redes de conmutación de paquetes. Estos dos últimos puntos cubren aspectos que resultan básicos para el encaminamiento en redes de tipo internet.

12.1. ENCAMINAMIENTO EN REDES DE CONMUTACIÓN DE CIRCUITOS

En una red grande de conmutación de circuitos como, por ejemplo, la red telefónica de larga distancia de AT&T, muchas de las conexiones de circuitos necesitan una ruta que atraviese más de un conmutador. Cuando se establece una llamada, la red debe encontrar una ruta desde el abonado llamante hasta el abonado llamado que pase a través de varios conmutadores y enlaces. Existen dos requisitos fundamentales para la arquitectura de red que tienen efecto sobre la estrategia de encaminamiento: eficiencia y flexibilidad. En primer lugar, es deseable minimizar la cantidad de equipos (conmutadores y enlaces) en la red, teniendo en cuenta que debemos ser capaces de gestionar toda la carga esperada. Las necesidades de carga se expresan usualmente en términos de tráfico en horas punta, lo cual se refiere, sencillamente, a la carga promedio esperada durante los periodos de más actividad a lo largo del día. Desde un punto de vista práctico, es necesario ser capaz de gestionar esta cantidad de tráfico; desde el punto de vista del coste, sería deseable gestionar esta carga con el menor equipamiento posible. Otro requisito es la flexibilidad. Aunque la red se puede dimensionar teniendo en cuenta el tráfico en horas punta, es posible que la carga supere temporalmente este nivel (por ejemplo, durante una gran tormenta). Puede darse también el caso de que, ocasionalmente, los conmutadores y las líneas fallen y se encuentren momentáneamente inaccesibles (puede que, desgraciadamente, coincidiendo con la propia tormenta). Sería deseable, por tanto, que la red proporcionase un nivel razonable de servicio incluso bajo tales circunstancias.

El aspecto clave de diseño que determina la naturaleza del compromiso entre eficiencia y flexibilidad es la estrategia de encaminamiento. Tradicionalmente, la función de encaminamiento en redes públicas de telecomunicaciones ha sido bastante simple. Esencialmente, los conmutadores de

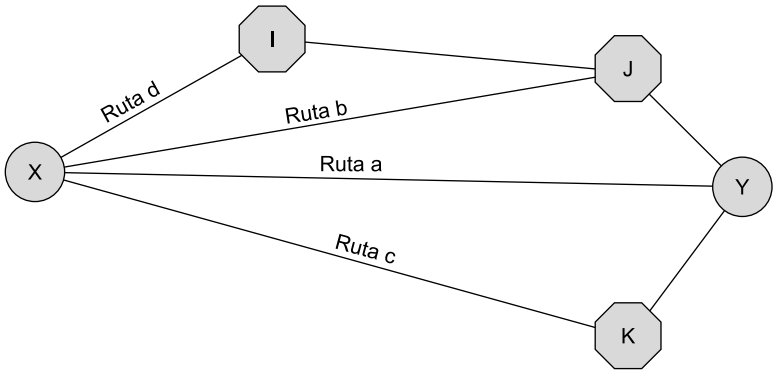
una red se organizaban en una estructura en árbol o jerarquía, estableciéndose una ruta a través del árbol, comenzando en el abonado llamante, hasta el primer nodo común, y después hasta el abonado llamado. Para proporcionar cierta flexibilidad a la red, se incluían en el árbol enlaces de alta capacidad adicionales para conectar entre sí centrales con altos volúmenes de tráfico. En general, esta aproximación es de naturaleza estática. La incorporación de enlaces de alta capacidad proporciona redundancia y capacidad extra, pero persisten las limitaciones en términos de eficiencia y de flexibilidad. Dado que este esquema de encaminamiento no es capaz de adaptarse a condiciones cambiantes, la red debe diseñarse para dar servicio en condiciones típicas de alta carga. Para ofrecer un ejemplo de los problemas a los que da lugar esta aproximación, téngase en cuenta que las horas punta para el tráfico este-oeste no coinciden con las del tráfico norte-sur y plantean, además, diferentes demandas al sistema. Es difícil analizar los efectos de estas variables, que pueden dar lugar a un sobredimensionamiento y, en consecuencia, provocar ineficiencia. En términos de flexibilidad, la estructura jerárquica fija con enlaces adicionales puede responder pobremente ante la ocurrencia de fallos. En general, la consecuencia de un fallo en estos casos es la aparición de una congestión local importante cerca del lugar donde se origina el fallo.

Para hacer frente a la creciente demanda de las redes públicas de telecomunicaciones, la práctica totalidad de los proveedores han pasado de una aproximación jerárquica estática a la adopción de una aproximación dinámica. En un esquema de encaminamiento dinámico las decisiones de encaminamiento están influenciadas en cada instante de tiempo por las condiciones de tráfico actuales. Generalmente, los nodos de conmutación de circuitos mantienen una relación de igual a igual entre sí, en lugar de una jerárquica como la presente en el esquema estático. Todos los nodos están capacitados para realizar las mismas funciones. Esta arquitectura de encaminamiento es más compleja y, a la vez, más flexible. Más compleja porque la arquitectura no proporciona una ruta o conjunto de rutas «natural» basándose en la estructura jerárquica, pero al mismo tiempo es más flexible debido a que hay más rutas alternativas.

Como ejemplo, veamos una forma de encaminamiento en redes de conmutación de circuitos llamada **encaminamiento alternativo**. La base de los esquemas de encaminamiento alternativo reside en que las posibles rutas entre dos centrales finales se encuentran predefinidas, siendo responsabilidad del conmutador origen seleccionar el camino adecuado para cada llamada. Cada conmutador dispone de un conjunto de rutas prefijadas, en orden de preferencia, para cada destino; si existe una conexión directa entre dos conmutadores, ésta suele ser la elección preferida; si no está disponible esta línea se prueba con la segunda alternativa, y así sucesivamente. Las secuencias de encaminamiento (conjunto de rutas intentadas) reflejan un análisis basado en patrones de tráfico conocidos y se diseñan para optimizar la utilización de los recursos de la red.

Si sólo se define una secuencia de encaminamiento para cada pareja origen-destino, el esquema se conoce como esquema de encaminamiento alternativo fijo. No obstante, es más frecuente el uso de un esquema de encaminamiento alternativo dinámico, en el cual se utiliza un conjunto diferente de rutas preplanificadas en instantes distintos de tiempo, con objeto de aprovechar las distintas condiciones de tráfico en las diferentes franjas horarias y en los distintos periodos de un día. En consecuencia, la decisión de encaminamiento se basa tanto en el estado del tráfico actual (una ruta se descartará si está ocupada) como en patrones de tráfico conocidos (que determinan la secuencia de rutas a considerar).

En la Figura 12.1 se muestra un ejemplo sencillo. El conmutador origen, X, tiene cuatro posibles rutas hacia el conmutador destino, Y. Siempre se intentará en primer lugar la ruta directa *a*; si este enlace no está disponible (ocupado o fuera de servicio), se intentarán las otras rutas en un orden dado dependiendo de la hora de que se trate. Por ejemplo, durante las mañanas del fin de semana la siguiente ruta en probarse será la *b*.



(a) Topología

Periodo de tiempo	Primera ruta	Segunda ruta	Tercera ruta	Cuarta y última ruta
Mañana	a	b	c	d
Tarde	a	d	b	c
Noche	a	d	c	b
Fin de semana	a	c	b	d

(b) Tabla de encaminamiento

Figura 12.1. Rutas alternativas desde la central final X hasta la central final Y.

12.2. ENCAMINAMIENTO EN REDES DE CONMUTACIÓN DE PAQUETES

Uno de los aspectos más complejos y cruciales del diseño de redes de conmutación de paquetes es el relativo al encaminamiento. Este apartado comienza con una revisión de las principales características que se pueden usar para clasificar las estrategias de encaminamiento. Tras esto se discutirán algunos esquemas concretos.

Los principios descritos en esta sección son también aplicables al encaminamiento en la interconexión de redes, discutida en la Parte V del texto.

CARACTERÍSTICAS

La función principal de una red de conmutación de paquetes es aceptar paquetes procedentes de una estación emisora y enviarlos hacia una estación destino. Para ello se debe determinar una ruta a través de la red, siendo posible generalmente la existencia de más de una. Así pues, se debe realizar una función de encaminamiento, entre cuyos requisitos se encuentran los siguientes:

- Exactitud
- Simplicidad
- Robustez
- Estabilidad
- Imparcialidad
- Optimización
- Eficiencia

Las dos primeras características mencionadas se explican por sí mismas. La robustez está relacionada con la habilidad de la red para enviar paquetes de alguna forma ante la aparición de sobrecargas y fallos localizados. Idealmente, la red puede reaccionar ante estas contingencias sin sufrir pérdidas de paquetes o caída de circuitos virtuales. No obstante, la robustez puede implicar cierta inestabilidad. Las técnicas que reaccionan ante condiciones cambiantes presentan una tendencia no deseable a reaccionar demasiado lentamente ante determinados eventos o a experimentar oscilaciones inestables de una situación extrema a otra. Por ejemplo, la red puede reaccionar ante la aparición de congestión en un área desplazando la mayor parte de la carga hacia una segunda zona. Ahora será la segunda región la que estará sobrecargada y la primera infrautilizada, produciéndose un segundo desplazamiento del tráfico. Durante estos desplazamientos puede ocurrir que los paquetes viajen en bucles a través de la red.

También existe un compromiso entre la característica de imparcialidad y el hecho de que el encaminamiento trate de ser óptimo. Algunos criterios de funcionamiento pueden dar prioridad al intercambio de paquetes entre estaciones vecinas frente al intercambio realizado entre estaciones distantes, lo cual puede maximizar la eficiencia promedio pero será injusto para aquella estación que necesite comunicar principalmente con estaciones lejanas.

Finalmente, una técnica de encaminamiento implica cierto coste de procesamiento en cada nodo y, en ocasiones, también un coste en la transmisión, impidiéndose en ambos casos el funcionamiento eficiente de la red. Este coste debe ser inferior a los beneficios obtenidos por el uso de una métrica razonable, como la mejora de la robustez o la imparcialidad.

Con estos requisitos en mente estamos en condiciones de evaluar los distintos elementos de diseño involucrados en un esquema de encaminamiento. En la Tabla 12.1 se listan estos elementos. Algunos de ellos se solapan o dependen de otros, pero un estudio acerca de los mismos clarificará y permitirá organizar los conceptos de encaminamiento.

Tabla 12.1. Elementos de diseño en las técnicas de encaminamiento en redes de conmutación de paquetes.

Criterios de rendimiento	**Fuente de información de la red**
Número de saltos	Ninguna
Coste	Local
Retardo	Nodo adyacente
Eficiencia	Nodos a lo largo de la ruta
	Todos los nodos
Instante de decisión	
Paquete (datagrama)	**Tiempo de actualización de la información de la red**
Sesión (circuitos virtuales)	Continuo
	Periódico
Lugar de decisión	Cambio importante en la carga
Cada nodo (distribuido)	Cambio en la topología
Nodo central (centralizado)	
Nodo origen (fuente)	

Criterios de rendimiento

La elección de una ruta se fundamenta generalmente en algún criterio de rendimiento. El más simple consiste en elegir el camino con menor número de saltos (aquel que atraviesa el menor número

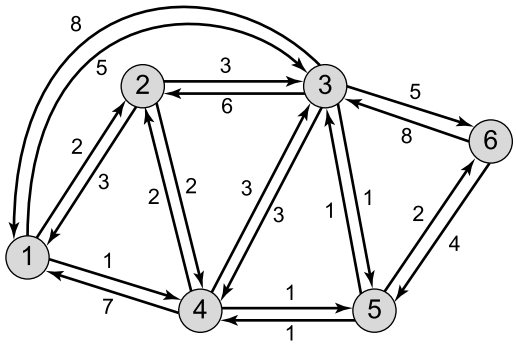


Figura 12.2. Ejemplo de red de conmutación de paquetes.

de nodos) a través de la red[1]. Éste es un criterio que se puede medir fácilmente y que debería minimizar el consumo de recursos de la red. Una generalización del criterio de menor número de saltos lo constituye el encaminamiento de mínimo coste. En este caso se asocia un coste a cada enlace y, para cualesquiera dos estaciones conectadas, se elige aquella ruta a través de la red que implique el coste total mínimo. Por ejemplo, en la Figura 12.2 se muestra una red en la que las dos líneas con flecha entre cada par de nodos representan un enlace entre ellos, y los números asociados indican el coste actual del enlace en cada sentido. El camino más corto (menor número de saltos) desde el nodo 1 hasta el 6 es 1-3-6 (coste = 5 + 5 = 10), pero el de mínimo coste es 1-4-5-6 (coste = 1 + 1 + 2 = 4). La asignación de los costes a los enlaces se hace en función de los objetivos de diseño; por ejemplo, el coste podría estar inversamente relacionado con la velocidad (es decir, a mayor velocidad menor coste) o con el retardo actual de la cola asociada al enlace. En el primer caso, la ruta de mínimo coste maximizaría la eficiencia, mientras que en el segundo minimizaría el retardo.

Tanto en la técnica de menor número de saltos como en la de mínimo coste, el algoritmo para determinar la ruta o camino óptimo entre dos estaciones es relativamente sencillo, siendo el tiempo de procesamiento aproximadamente el mismo en ambos casos. Dada su mayor flexibilidad, el criterio de mínimo coste es más utilizado que el de menor número de saltos.

Existen varios algoritmos de mínimo coste de uso común, los cuales se describen en la Sección 12.3.

Instante y lugar de decisión

Las decisiones de encaminamiento se realizan de acuerdo con algún criterio de rendimiento. Dos cuestiones importantes en la toma de esta decisión son el instante temporal y el lugar en que se toma la decisión.

El instante de decisión viene determinado por el hecho de que la decisión de encaminamiento se hace en base a un paquete o a un circuito virtual. Cuando la operación interna de la red se basa en datagramas, la decisión de encaminamiento se toma de forma individual para cada paquete. En

[1] El término *salto* se usa con cierta libertad en la bibliografía. La definición más común, usada en este texto, es que el número de saltos a lo largo de una ruta entre un origen y un destino dados es el número de nodos de la red (nodos de conmutación de paquetes, conmutadores ATM, dispositivos de encaminamiento, etc.) que encuentra un paquete a lo largo de dicha ruta. El número de saltos es igual a veces al número de enlaces, o terminales de grafo, atravesados. A partir de esta última definición se obtiene un valor superior en uno al conseguido mediante la definición aceptada en nuestro caso.

el caso de circuitos virtuales internos, la decisión sólo se realiza en el momento en que se establece un circuito virtual dado, de modo que, en el caso más sencillo, todos los paquetes siguientes que usan ese circuito virtual siguen la misma ruta. En redes más complejas, la red puede cambiar dinámicamente la ruta asignada a un circuito virtual particular en respuesta a condiciones cambiantes (por ejemplo, sobrecarga o fallos en una parte de la red).

El término *lugar de decisión* hace referencia al nodo o nodos en la red responsables de la decisión de encaminamiento. El más común es el encaminamiento distribuido, en el que cada nodo de la red tiene la responsabilidad de seleccionar un enlace de salida sobre el que llevar a cabo el envío de los paquetes a medida que éstos se reciben. En el encaminamiento centralizado, la decisión se toma por parte de algún nodo designado al respecto, como puede ser un centro de control de red. El peligro de esta última aproximación es que el fallo del centro de control puede bloquear el funcionamiento de la red; así pues, aunque la aproximación distribuida puede resultar más compleja es también más robusta. Una tercera alternativa empleada en algunas redes es la conocida como encaminamiento desde el origen. En este caso, es la estación origen y no los nodos de la red quien realmente toma la decisión de encaminamiento, comunicándosela a la red. Esto permite al usuario fijar una ruta a través de la red de acuerdo con criterios locales al mismo.

El instante y el lugar de decisión son variables de diseño independientes. Por ejemplo, supongamos que el lugar de decisión en la Figura 12.2 es cada nodo y que los valores especificados son los costes en un instante de tiempo dado, los cuales pueden cambiar. Un paquete desde el nodo 1 al 6 podría seguir la ruta 1-4-5-6, estando cada enlace de la ruta determinado localmente por el nodo transmisor. Supongamos ahora que los valores cambian de forma que 1-4-5-6 ya no es el camino óptimo. En una red de datagramas, el paquete siguiente puede seguir una ruta diferente, de nuevo determinada por cada nodo a lo largo del camino. En una red de circuitos virtuales, cada nodo recuerda la decisión de encaminamiento tomada cuando se estableció el circuito virtual, de modo que se limita a transmitir los paquetes sin tomar decisiones nuevas.

Fuente de información de la red y tiempo de actualización

La mayor parte de los esquemas de encaminamiento requieren que las decisiones se tomen en base al conocimiento de la topología de la red, la carga y el coste de los enlaces. Sorprendentemente, algunas estrategias, como la de inundaciones y el encaminamiento aleatorio (descritas más adelante), no hacen uso de ninguna información para la transmisión de los paquetes.

En el encaminamiento distribuido, en el que la decisión de encaminamiento se toma en cada uno de los nodos, éstos hacen uso de información local, como es el coste asociado a los distintos enlaces de salida; también pueden utilizar información de los nodos adyacentes (directamente conectados), como la congestión experimentada en ellos. Finalmente, existen algoritmos de uso común que permiten al nodo obtener información de todos los nodos de una potencial ruta de interés. En el caso del encaminamiento centralizado, el nodo central hace uso generalmente de información procedente de todos los nodos.

Un concepto relacionado es el de tiempo de actualización de la información, el cual es función de la fuente de información y de la estrategia de encaminamiento. Es evidente que si no se usa información (como en el método de inundaciones) no existe actualización. Si sólo se utiliza información local, la actualización es esencialmente continua, ya que un nodo individual conoce siempre sus condiciones locales actuales. Para el resto de categorías de fuentes de información (nodos adyacentes, todos los nodos), el tiempo de actualización depende de la estrategia de encaminamiento. Para una estrategia de encaminamiento estático, la información no se actualiza nunca,

mientras que para una técnica adaptable la actualización se lleva a cabo periódicamente a fin de posibilitar la adaptación de la decisión de encaminamiento a las condiciones cambiantes de la red.

Como cabe esperar, cuanto mayor sea la información disponible y más frecuentemente se actualice ésta, más probable será que las decisiones de encaminamiento tomadas por la red sean buenas. Eso sí, teniendo presente que la transmisión de esta información consume recursos de la red.

ESTRATEGIAS DE ENCAMINAMIENTO

Existen numerosas estrategias de encaminamiento para abordar las necesidades de encaminamiento en redes de conmutación de paquetes. Muchas de ellas son aplicables también al encaminamiento en la interconexión de redes, estudiada en la Parte V del texto. En este apartado se presentan cuatro estrategias principales: estática, inundaciones, aleatoria y adaptable.

Encaminamiento estático

En el encaminamiento estático se configura una única ruta permanente para cada par de nodos origen-destino en la red, pudiéndose utilizar para ello cualquiera de los algoritmos de encaminamiento de mínimo coste descritos en la Sección 12.3. Las rutas son fijas (al menos mientras lo sea la topología de la red), de modo que los costes de enlace usados para el diseño de las rutas no pueden estar basados en variables dinámicas como el tráfico, aunque sí podrían estarlo en tráfico esperado o en capacidad.

La Figura 12.3 sugiere cómo se pueden implementar rutas estáticas. Se crea una matriz de encaminamiento central, almacenada, por ejemplo, en un centro de control de red. Esta matriz especifica, para cada par de nodos origen-destino, la identidad del siguiente nodo en la ruta.

Obsérvese que no es necesario almacenar la ruta completa para cada par de nodos; es suficiente conocer, para cada pareja, cuál es el primer nodo en la ruta. Para comprender mejor este hecho, supongamos que la ruta de mínimo coste desde X hasta Y comienza con el enlace X-A. Llamemos R_1 al resto de la ruta, es decir, desde A hasta Y, y definamos R_2 como la ruta de mínimo coste de A a Y. Si el coste de R_1 es mayor que el de R_2, la ruta X-Y mejorará al usar R_2 en lugar de R_1. Si el coste de R_1 es menor que el de R_2, entonces esta última ruta no es la de mínimo coste desde A hasta Y; por tanto, $R_1 = R_2$. Así pues, en cada punto a lo largo del camino sólo es necesario conocer la identidad del nodo siguiente, no la ruta completa. En nuestro ejemplo, la ruta desde el nodo 1 al nodo 6 atraviesa en primer lugar el nodo 4. Consultando de nuevo la matriz, se observa que la ruta del nodo 4 al 6 atraviesa el nodo 5. Por último, la ruta desde el nodo 5 hasta el 6 es un enlace directo entre ambos. Por tanto, la ruta completa desde el nodo 1 al 6 es 1-4-5-6.

A partir de esta matriz se pueden crear y almacenar en cada nodo las tablas de encaminamiento asociadas. Siguiendo el razonamiento del párrafo anterior, cada nodo sólo necesitará almacenar una columna de la tabla de encaminamiento, indicándose en ella el nodo siguiente para cada destino.

En el encaminamiento estático no existe diferencia entre el uso de datagramas y de circuitos virtuales, ya que todos los paquetes procedentes de un origen dado y con un destino concreto siguen la misma ruta. La ventaja del encaminamiento estático es su simplicidad, además de su buen funcionamiento en redes fiables con carga estacionaria. Su desventaja, en cambio, radica en la falta de flexibilidad, ya que no reacciona ante fallos ni ante congestión en la red.

MATRIZ DE ENCAMINAMIENTO CENTRAL

Nodo origen

Nodo destino	1	2	3	4	5	6
1	—	1	5	2	4	5
2	2	—	5	2	4	5
3	4	3	—	5	3	5
4	4	4	5	—	4	5
5	4	4	5	5	—	5
6	4	4	5	5	6	—

Tabla del nodo 1

Destino	Nodo siguiente
2	2
3	4
4	4
5	4
6	4

Tabla del nodo 2

Destino	Nodo siguiente
1	1
3	3
4	4
5	4
6	4

Tabla del nodo 3

Destino	Nodo siguiente
1	5
2	5
4	5
5	5
6	5

Tabla del nodo 4

Destino	Nodo siguiente
1	2
2	2
3	5
5	5
6	5

Tabla del nodo 5

Destino	Nodo siguiente
1	4
2	4
3	3
4	4
6	6

Tabla del nodo 6

Destino	Nodo siguiente
1	5
2	5
3	5
4	5
5	5

Figura 12.3. Encaminamiento estático (haciendo uso de la Figura 12.2).

Una mejora al encaminamiento estático, que soportaría la no disponibilidad temporal de nodos y enlaces, consiste en la especificación de nodos siguientes alternativos para cada dirección. Por ejemplo, los nodos alternativos en la tabla del nodo 1 serían 4, 3, 2, 3, 3.

Inundaciones

Otra técnica de encaminamiento sencilla es la de inundaciones, la cual no precisa de ninguna información sobre la red y funciona como sigue. Un nodo origen envía un paquete a todos sus nodos vecinos, los cuales, a su vez, lo transmiten sobre todos los enlaces de salida excepto por el que llegó. Por ejemplo, si el nodo 1 de la Figura 12.2 tiene que enviar un paquete al nodo 6, transmite una copia (con la dirección de destino de 6) a los nodos 2, 3 y 4. El nodo 2 enviará una copia a los nodos 3 y 4; el nodo 4 enviará, a su vez, una copia a los nodos 2, 3 y 5; y así sucesivamente. Dado que, eventualmente, el nodo 6 recibirá varias copias del paquete, éste debe contener un identificador único (por ejemplo, nodo origen y número de secuencia o número de circuito virtual y número de secuencia) para que el nodo destino pueda quedarse con una sola copia y descartar el resto.

A menos que se haga algo para cesar las continuas retransmisiones de paquetes, el número de éstos en circulación para un mismo paquete origen crece sin límite. Una forma de prevenir estas

retransmisiones consiste en que cada nodo recuerde la identidad de los paquetes que ha retransmitido con anterioridad, de manera que se rechazan copias duplicadas. Una técnica más sencilla consiste en incluir un campo de cuenta de saltos en cada paquete. Este contador puede ponerse inicialmente a un valor máximo, como es por ejemplo el diámetro de la red (longitud de la ruta de menor número de saltos más larga a través de la red)[2]. Cada vez que un nodo transmite un paquete decrementa la cuenta en uno, de modo que cuando el contador alcanza el valor cero se elimina el paquete de la red.

Un ejemplo de esta última técnica se muestra en la Figura 12.4. Supongamos que se envía un paquete desde el nodo 1 al nodo 6 y se le asigna una cuenta de saltos igual a 3. En el primer salto se crean tres copias del paquete; en el segundo salto de estas copias se crea un total de nueve copias. Una de estas copias alcanza el nodo 6, quien, al detectar que el destino es él, no la retransmite. Sin embargo, los otros nodos generan un total de 22 nuevas copias en el tercer y último salto. Obsérvese que si un nodo no guarda el identificador del paquete puede generar múltiples copias

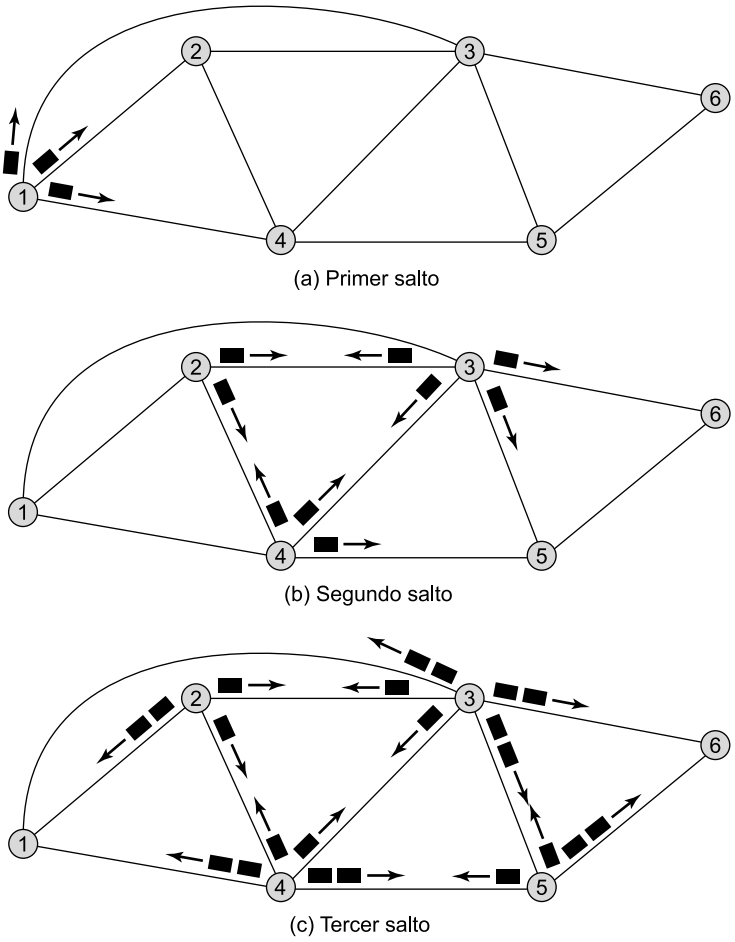


Figura 12.4. Ejemplo de inundaciones (número de saltos = 3).

[2] Para cada pareja de sistemas finales conectados a la red existe una ruta de menor número de saltos, denominándose diámetro de la red a la longitud de la ruta más larga de entre todas las de menor número de saltos.

en este tercer paso. Todos los paquetes recibidos tras el tercer salto son eliminados, habiéndose recibido en el nodo 6 un total de cuatro copias adicionales del paquete.

La técnica de inundaciones presenta tres propiedades importantes:

- Se prueban todos los posibles caminos entre los nodos origen y destino. De este modo, independientemente de lo que pueda sucederle a un nodo o a un enlace, se garantiza la recepción del paquete siempre que exista, al menos, una ruta entre el origen y el destino.
- Dado que se prueban todos los caminos, al menos una copia del paquete a recibir en el destino habrá usado una ruta de menor número de saltos.
- Se visitan todos los nodos que están directa o indirectamente conectados al nodo origen.

Por la primera propiedad, la técnica de inundaciones resulta muy robusta y puede ser usada para enviar mensajes de alta prioridad. Un ejemplo de aplicación es una red militar que puede sufrir daños importantes. Por la segunda propiedad, la técnica de inundaciones podría emplearse inicialmente para establecer la ruta para un circuito virtual. La tercera propiedad sugiere que la técnica de inundaciones puede resultar útil para llevar a cabo la propagación de información relevante para todos los nodos; ya se verá que se utiliza en algunos esquemas para la propagación de información de encaminamiento.

La principal desventaja de la técnica de inundaciones es la gran cantidad de tráfico que genera, directamente proporcional a la conectividad de la red.

Encaminamiento aleatorio

La técnica de encaminamiento aleatorio presenta, con menor tráfico, la sencillez y robustez de la técnica de inundaciones. En este esquema, un nodo selecciona un único camino de salida para retransmitir un paquete entrante; el enlace de salida se elige de forma aleatoria, excluyendo el enlace por el que llegó el paquete. Si todos los enlaces son igualmente probables de ser elegidos, una implementación sencilla consistiría en seleccionarlos de forma alternada.

Una mejora a esta técnica consiste en asignar una probabilidad a cada uno de los enlaces de salida y llevar a cabo la selección de acuerdo con estas probabilidades. La probabilidad se puede basar en la velocidad de datos, en cuyo caso se tiene

$$P_i = \frac{R_i}{\sum_j R_j}$$

donde

P_i = probabilidad de seleccionar el enlace i.

R_i = velocidad del enlace i.

La suma se realiza para todos los enlaces de salida candidatos. Este esquema proporciona una distribución del tráfico adecuada. Obsérvese que las probabilidades también podrían estar basadas en costes de enlace fijos.

Como en el caso de la técnica de inundaciones, el encaminamiento aleatorio no necesita el uso de información sobre la red. Dado que la ruta se elige de forma aleatoria, ésta no corresponderá en general con la de mínimo coste ni con la de menor número de saltos. Por tanto, la red debe transportar un tráfico superior al óptimo, aunque inferior al de la técnica de inundaciones.

Encaminamiento adaptable

Prácticamente en todas las redes de conmutación de paquetes se utiliza algún tipo de técnica de encaminamiento adaptable; es decir, las decisiones de encaminamiento cambian en la medida que lo hacen las condiciones de la red. Las principales condiciones que influyen en las decisiones de encaminamiento son:

- **Fallos:** cuando un nodo o una línea troncal fallan, no pueden volver a ser usados como parte de una ruta.
- **Congestión:** cuando una parte de la red sufre una congestión importante, es deseable encaminar los paquetes de forma que se rodee la zona congestionada, en lugar de realizar el encaminamiento a través de ella.

Para hacer posible el encaminamiento adaptable es necesario que los nodos intercambien información acerca del estado de la red. El uso de la técnica de encaminamiento adaptable presenta varias desventajas en comparación con el encaminamiento estático:

- La decisión de encaminamiento es más compleja, por lo que aumenta el coste de procesamiento en los nodos de la red.
- En la mayor parte de los casos, las estrategias adaptables dependen de la información de estado obtenida en una parte de la red pero que es utilizada en otra. Existe un compromiso entre la calidad de la información y la cantidad de datos suplementarios o redundancia utilizada. Cuanta más información se intercambia y más frecuentemente se hace, mejores serán las decisiones de encaminamiento tomadas en cada nodo. Por otro lado, esta información constituye en sí misma tráfico adicional sobre la red, lo que supone cierta degradación de las prestaciones de ésta.
- Una estrategia adaptable puede reaccionar demasiado rápidamente, provocando oscilaciones y causando congestión, o demasiado lentamente, en cuyo caso no es válida.

A pesar de estos peligros reales, las estrategias de encaminamiento adaptable son, con mucho, las más utilizadas por dos razones:

- El usuario de la red percibe que las prestaciones mejoran con el uso de estas técnicas.
- Como se discutirá en el Capítulo 13, una estrategia de encaminamiento adaptable puede resultar de ayuda en el control de la congestión: dado que este tipo de técnica tiende a compensar la carga, puede retrasar la aparición de situaciones graves de congestión.

Dependiendo de la validez del diseño y de la naturaleza del tráfico, estas ventajas se pueden constatar o no debido a la complejidad para lograr un funcionamiento correcto. Como demostración de este hecho, la mayor parte de las redes de conmutación de paquetes, como ARPANET y sus sucesoras y varias redes comerciales, han sufrido al menos una revisión en sus técnicas de encaminamiento.

Una clasificación adecuada de las estrategias de encaminamiento adaptable es la realizada de acuerdo con la fuente de la información: local, nodos adyacentes o todos los nodos. Un ejemplo de técnica adaptable basada sólo en información local es aquella en la que cada nodo encamina cada paquete recibido por la línea de salida cuya cola asociada Q sea menor, lo que haría que se compensase la carga entre las distintas líneas de salida. Sin embargo, puede que algunos enlaces de salida no lleven al destino adecuado, por lo que se podría mejorar la técnica, como en el caso del encaminamiento aleatorio, teniendo en consideración la dirección deseada. En este caso, cada enlace de salida tendría un peso B_i para cada destino i. Para cada paquete recibido con destino el

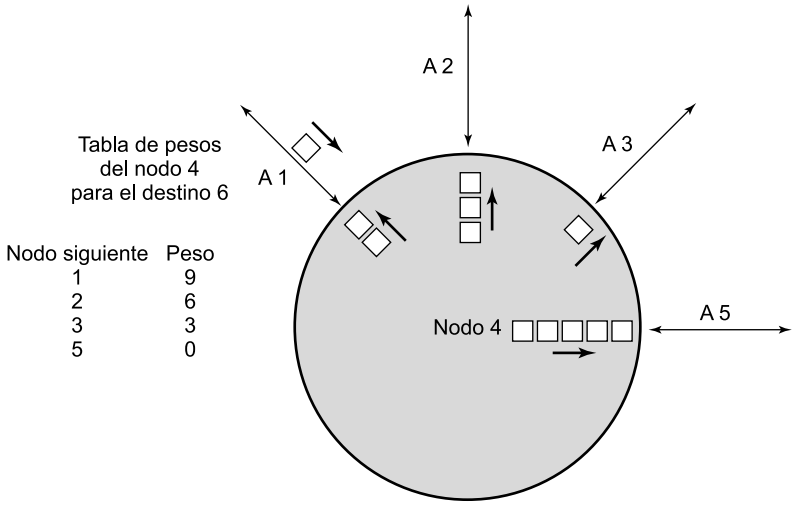


Figura 12.5. Ejemplo de encaminamiento adaptable aislado.

nodo *i*, el nodo intermedio elegirá aquella línea que minimice $Q + B_i$, de manera que los paquetes se envían en la dirección correcta considerando los retardos provocados por el tráfico.

Como ejemplo, en la Figura 12.5 se muestra el estado del nodo 4 de la Figura 12.2 en un instante de tiempo dado. Este nodo tiene sendos enlaces a otros cuatro nodos. Al recibirse varios paquetes se produce un exceso, de forma que se crea una cola de paquetes para cada una de las líneas de salida. ¿Hacia qué línea se debería encaminar un paquete recibido desde el nodo 1 con destino al 6? De acuerdo con las longitudes de las colas y la tabla de pesos (B_6) para cada enlace de salida, el valor mínimo de $Q + B_6$ es 4, correspondiente al enlace hacia el nodo 3. Por tanto, el nodo 4 encaminará el paquete hacia dicho nodo.

Los esquemas adaptables basados sólo en información local son raramente utilizados, puesto que no explotan con facilidad la información disponible. Las estrategias basadas en el uso de la información procedente de los nodos adyacentes o de todos los nodos se utilizan más debido a la mejor información acerca de los retardos en los nodos de que se dispone en estos casos. Estas técnicas adaptables pueden ser distribuidas o centralizadas. En el primer caso, cada nodo intercambia información de retardo con otros nodos, de modo que cada nodo trata de estimar el retardo a través de la red a partir de la información recibida y en base a un algoritmo de encaminamiento de mínimo coste. En el caso de una técnica centralizada, cada nodo informa sobre su estado de retardo a un nodo central, quien diseña las rutas de acuerdo con esta información recibida y devuelve la información de encaminamiento a los nodos.

EJEMPLOS

En este apartado se estudiarán varios ejemplos de estrategias de encaminamiento. Todas ellas fueron desarrolladas para ARPANET, que es una red de conmutación de paquetes predecesora de la actual Internet. Resulta instructivo examinar estas estrategias por varias razones. Primero, porque éstas y otras técnicas similares se usan también en otras redes de conmutación de paquetes, incluyendo varias de las que componen Internet. En segundo lugar, hay que decir que los esquemas de encaminamiento basados en el trabajo de ARPANET se han usado también en la interconexión

de redes en Internet y en redes privadas. Por último, porque el esquema de encaminamiento de ARPANET evolucionó de una manera que aclara algunos de los aspectos clave en el diseño de los algoritmos de encaminamiento.

Primera generación

El algoritmo de encaminamiento original, diseñado en 1969, era un algoritmo adaptable distribuido que hacía uso de la estimación de los retardos como criterio de rendimiento y de una versión del algoritmo de Bellman-Ford (*véase* Sección 12.3). Para este algoritmo, cada nodo mantiene dos vectores:

$$D_i = \begin{bmatrix} d_{i1} \\ \vdots \\ d_{iN} \end{bmatrix} \qquad S_i = \begin{bmatrix} s_{i1} \\ \vdots \\ s_{iN} \end{bmatrix}$$

donde

D_i = vector de retardo para el nodo i.

d_{ij} = estimación actual del retardo mínimo desde el nodo i al nodo j ($d_{ii} = 0$).

N = número de nodos en la red.

S_i = vector de nodos sucesores para el nodo i.

s_{ij} = nodo siguiente en la ruta actual de mínimo retardo de i a j.

Periódicamente (cada 128 ms), cada nodo intercambia su vector de retardo con todos sus vecinos. A partir de todos los vectores de retardo recibidos, un nodo k actualiza sus dos vectores como sigue:

$$d_{kj} = \min_{i \in A} [d_{ij} + l_{ki}]$$

$s_{kj} = i$, siendo i el que minimiza la expresión anterior

donde

A = conjunto de nodos vecinos de k.

l_{ki} = estimación actual del retardo desde el nodo k al nodo i.

En la Figura 12.6 se muestra un ejemplo del algoritmo original de ARPANET, usando la red de la Figura 12.7. Ésta es la misma red que la de la Figura 12.2 pero con diferentes costes asociados a los enlaces (y suponiendo el mismo coste en ambos sentidos del enlace). En la Figura 12.6a se muestra la tabla de encaminamiento del nodo 1 en un instante de tiempo que refleja los costes asociados a los enlaces de la Figura 12.7. Para cada destino se especifica un retardo y el nodo siguiente en la ruta que lo produce. En algún momento, los costes de los enlaces cambian a los valores indicados en la Figura 12.2. Supuesto que los vecinos del nodo 1 (nodos 2, 3 y 4) conociesen el cambio antes que él, cada uno de estos nodos actualizará su vector de retardo y enviará una copia a todos sus vecinos, incluyendo el nodo 1 (*véase* Figura 12.6b). El nodo 1 desecha su tabla de encaminamiento y construye una nueva basándose en los vectores de retardo recibidos y en la propia estimación que él hace del retardo para cada uno de los enlaces de salida a sus vecinos. El resultado obtenido se muestra en la Figura 12.6c.

El retardo de enlace estimado no es más que el tamaño o longitud de la cola para el enlace en cuestión. Así, con la construcción de una nueva tabla de encaminamiento el nodo tiende a favore-

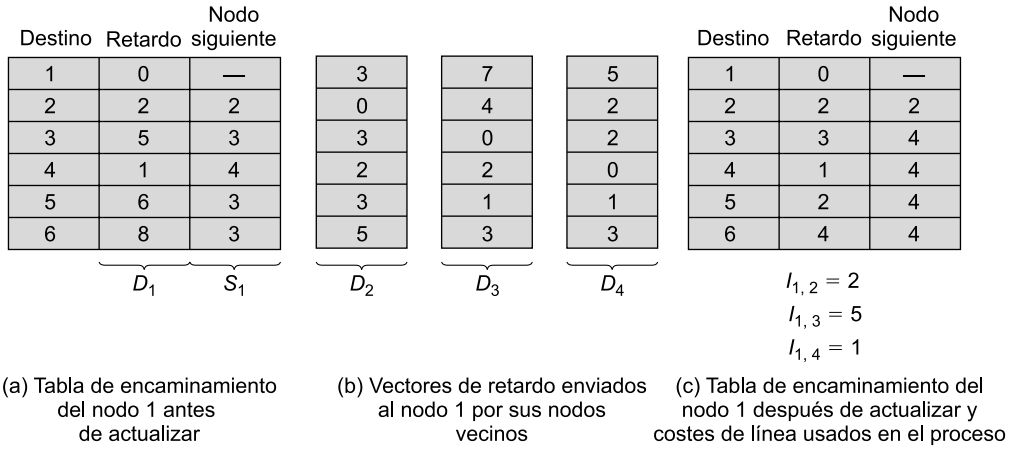


Figura 12.6. Algoritmo de encaminamiento original de ARPANET.

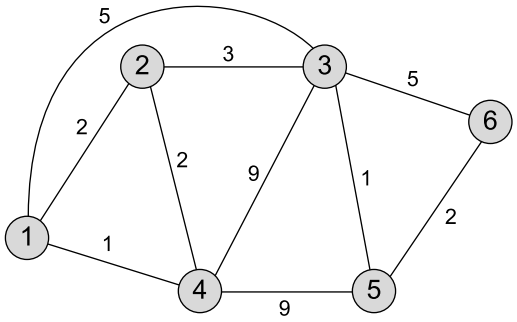


Figura 12.7. Red para el ejemplo de la Figura 12.6a.

cer aquellos enlaces con menores colas, lo que compensa la carga entre las distintas líneas de salida. Sin embargo, dado que el tamaño de las colas varía rápidamente a lo largo del tiempo, la percepción distribuida de la ruta más corta podría cambiar mientras un paquete se encuentra en tránsito. Esto podría provocar una situación en la que un paquete se encamina hacia un área de baja congestión en lugar de hacia el destino.

Segunda generación

Tras años de experiencia y algunas modificaciones sin importancia, el algoritmo de encaminamiento original se reemplazó en 1979 por otro bastante diferente [MCQU80]. Los principales inconvenientes del antiguo algoritmo eran los siguientes:

- No se consideraba la velocidad de las líneas sino sólo su tamaño de cola, por lo que a las líneas de alta capacidad no se les daba el tratamiento de favor que merecían.
- El tamaño de las colas es, en cualquier caso, una medida artificial del retardo, ya que se consume un cierto tiempo de procesamiento desde que el paquete se recibe en un nodo hasta que es puesto en cola.

- El algoritmo no era demasiado preciso; de hecho, su respuesta era muy lenta ante aumentos en la congestión y en el retardo.

El nuevo algoritmo es también adaptable distribuido en el que se hace uso del retardo como criterio de rendimiento, pero las diferencias son significativas. En lugar de usar la longitud de la cola como indicador del retardo, éste se mide directamente como sigue. A cada paquete recibido en un nodo se le coloca un sello o marca de tiempo indicando el instante temporal en que llegó. También se almacena el instante en que se transmite. Si se recibe una confirmación positiva, el retardo se calcula como el tiempo de salida menos el de llegada más el tiempo de transmisión y el de propagación. Para ello, el nodo debe conocer la velocidad del enlace y el tiempo de propagación. En cambio, si se recibe una confirmación negativa, se actualiza el tiempo de salida y el nodo vuelve a intentarlo hasta que se consigue con éxito una medida del retardo de transmisión.

El nodo calcula el retardo medio de cada enlace de salida cada 10 segundos. Si se producen cambios significativos en el valor obtenido, se envía la información a los demás nodos mediante el algoritmo de inundaciones. Cada nodo mantiene una estimación del retardo de cada enlace de la red, de modo que cuando recibe nueva información se actualiza la tabla de encaminamiento haciendo uso del algoritmo de Dijkstra (*véase* Sección 12.3).

Tercera generación

La experiencia con este nuevo esquema demostró que era más adecuado y estable que el anterior. El coste derivado del empleo de la técnica de inundaciones era moderado, ya que cada nodo la llevaba a cabo cada 10 segundos; sin embargo, se observó un problema en el funcionamiento de esta nueva estrategia a medida que aumentaba el tráfico en la red, por lo que fue revisada en 1987 [KHAN89].

El problema de la segunda estrategia consistía en la suposición de que el retardo de paquetes estimado para un enlace es un buen indicador del retardo de enlace, una vez que todos los nodos realizan el encaminamiento de su tráfico basándose en dicho retardo. Este mecanismo de encaminamiento resulta efectivo sólo si existe alguna correlación entre los valores estimados y los realmente experimentados una vez realizado el encaminamiento. Esta correlación tiende a ser mayor cuando el tráfico es bajo o moderado, pero cuando existe alta carga la correlación es pequeña. Por tanto, inmediatamente después de que todos los nodos hayan actualizado las tablas, éstas quedan obsoletas.

Como ejemplo, considérese una red consistente en dos regiones con sólo dos enlaces, A y B, que las conectan (*véase* Figura 12.8). Cualquier ruta entre dos nodos situados en regiones diferentes debe atravesar uno de estos enlaces. Supóngase una situación tal que la mayor parte del tráfico lo soporta la línea A. Esto implicará que el retardo en dicha línea es elevado, comunicándose este hecho al resto de los nodos en el siguiente instante de tiempo. Esta actualización se recibirá en todos los nodos aproximadamente al mismo tiempo, actualizándose inmediatamente sus tablas de encaminamiento. Es probable que este nuevo retardo para el enlace A sea lo suficientemente elevado para hacer que el enlace B sea ahora el elegido por la mayoría de las rutas, si no todas, entre ambas regiones. Dado que todos los nodos actualizan sus tablas al mismo tiempo, la mayor parte del tráfico entre las dos regiones se desplaza simultáneamente hacia la línea B. Esto provocará que sea ahora esta línea la que presente un retardo elevado, por lo que el tráfico se desplazará de nuevo hacia la línea A. Esta oscilación persistirá mientras lo haga el volumen de tráfico.

Existen varias razones por las que dicha oscilación resulta indeseable:

- Una parte importante de la capacidad disponible no se utiliza precisamente cuando más se necesita: en condiciones de alta carga.

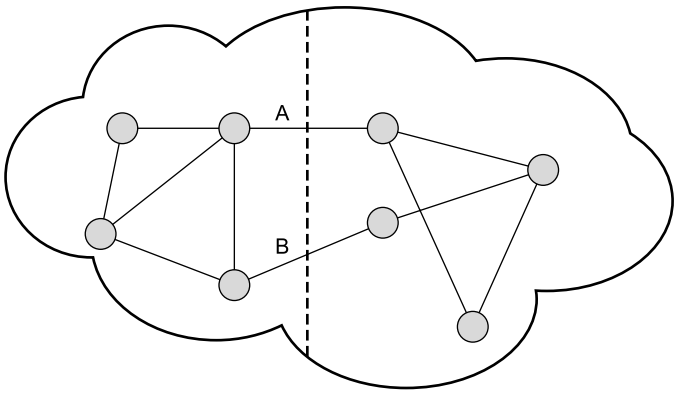


Figura 12.8. Red de conmutación de paquetes sujeta a oscilaciones.

- La utilización excesiva de algunos enlaces puede provocar congestión en la red (esto se verá cuando se estudie la congestión en el Capítulo 13).
- Las oscilaciones en los valores de retardo obtenidos hacen necesaria una actualización más frecuente de las tablas de encaminamiento. Este hecho incrementa el tráfico en la red justo cuando ésta ya presenta alta carga.

Los diseñadores de ARPANET concluyeron que el problema radicaba en el hecho de que todos los nodos estaban tratando de obtener la ruta óptima para todos los destinos, lo que provocaba conflictos. Se concluyó que, para alta carga, el objetivo del encaminamiento debería consistir en la obtención de una ruta promedio, en lugar de intentar la determinación de todos los caminos mejores.

Los diseñadores decidieron que era innecesario cambiar todo el algoritmo; el cambio de la función que determinaba el coste de los enlaces bastaba para evitar las oscilaciones en el encaminamiento y reducir su coste. El cálculo comienza midiendo el retardo medio en los últimos 10 segundos. Este valor se transforma como se indica a continuación:

1. Haciendo uso de un sencillo modelo de colas con un único servidor, el retardo medido se transforma en una estimación de la utilización de la línea. Por teoría de colas, la utilización se puede expresar en función del retardo como sigue:

$$\rho = \frac{2(T_s - T)}{T_s - 2T}$$

donde

ρ = utilización del enlace.

T = retardo medido.

T_s = tiempo de servicio.

El tiempo de servicio se hace igual al tamaño medio de los paquetes en la red (600 bits) dividido entre la velocidad de la línea.

2. El resultado se suaviza promediándolo con la utilización estimada previamente:

$$U(n + 1) = 0{,}5 \times \rho(n + 1) + 0{,}5 \times U(n)$$

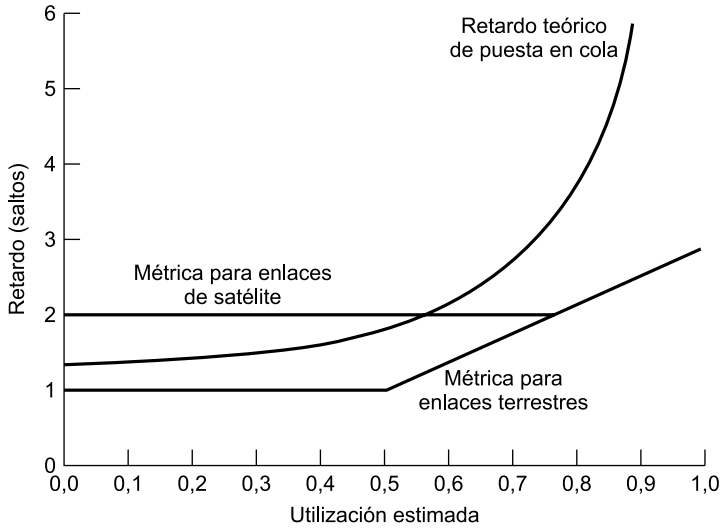


Figura 12.9. Métricas de retardo en ARPANET.

donde

$U(n)$ = utilización media calculada en el instante de muestreo n.

$\rho(n)$ = utilización del enlace en el instante de tiempo n.

El valor promedio incrementa el periodo de las oscilaciones en el encaminamiento, lo que reduce el coste adicional de este último.

3. El coste del enlace se establece como una función de la utilización media, pensada para proporcionar una estimación razonable del coste sin provocar oscilación. En la Figura 12.9 se indica la forma de convertir la estimación de la utilización en un valor de coste, valor que se obtiene a partir del retardo.

En la Figura 12.9 mencionada se normaliza el retardo al valor alcanzado en una línea desocupada, el cual corresponde al tiempo de propagación más el tiempo de transmisión. Cada curva en la figura indica la forma en que el retardo real depende de la utilización; el incremento en el retardo se debe al retardo de cola en el nodo. Para el nuevo algoritmo, el coste se mantiene al valor mínimo hasta que se alcanza un nivel de utilización dado, lo que tiene el efecto de reducir el coste del encaminamiento cuando el tráfico es reducido. Por encima de un cierto nivel de utilización, se permite que el coste alcance un valor máximo igual a tres veces el valor mínimo. El efecto de este valor máximo es establecer que el tráfico no debe ser encaminado alrededor de una línea con alta carga más que en dos saltos adicionales.

Obsérvese que el umbral mínimo es superior para enlaces satélite, lo que potencia el uso de los enlaces terrestres para condiciones de baja carga, dado que éstos presentan un retardo de propagación inferior. Nótese también que la curva de retardo real es mucho más pronunciada que las curvas de transformación para altos niveles de utilización. Esta pendiente en el coste del enlace provoca que el tráfico en un enlace se distribuya, lo que causa la aparición de oscilaciones en el encaminamiento.

En resumen, la función de coste estudiada está más orientada a la utilización que al retardo. La función actúa de forma similar a una métrica basada en retardo cuando la carga es baja y a una métrica basada en la capacidad en condiciones de alta carga.

12.3. ALGORITMOS DE MÍNIMO COSTE

Prácticamente todas las redes de conmutación de paquetes y todas las redes de tipo internet basan sus decisiones de encaminamiento en algún criterio de mínimo coste. Si el criterio consiste en minimizar el número de saltos, cada enlace tendrá asociado un valor igual a 1. Normalmente, el valor asociado al enlace es inversamente proporcional a su capacidad, proporcional a su carga actual o alguna combinación de ellos. En cualquier caso, el coste de las líneas se emplea como entrada a un algoritmo de encaminamiento de mínimo coste, que establece que:

> Dada una red de nodos conectados entre sí por enlaces bidireccionales, donde cada enlace tiene un coste asociado en cada sentido, se define el coste de una ruta entre dos nodos como la suma de los costes de los enlaces atravesados. Así, para cada par de nodos se obtiene el camino de mínimo coste.

Obsérvese que el coste de un enlace puede ser diferente para cada uno de los dos sentidos. Esto sería cierto, por ejemplo, si el coste de un enlace fuese igual a la longitud de la cola de paquetes esperando ser transmitidos sobre el enlace por cada uno de los dos nodos.

La mayor parte de los algoritmos de encaminamiento de mínimo coste utilizados en las redes de conmutación de paquetes y en las redes internet son variantes de uno de los dos algoritmos más comunes: el de Dijkstra y el de Bellman-Ford. Este apartado presenta una breve descripción de ambos.

ALGORITMO DE DIJKSTRA

El algoritmo de Dijkstra [DIJK59] se puede enunciar como sigue: encontrar las rutas más cortas entre un nodo origen dado y todos los demás nodos, desarrollando los caminos en orden creciente de longitud. El algoritmo actúa en etapas. Tras el paso o etapa k-ésima se han determinado los caminos más cortos a los k nodos más cercanos (de menor coste) al nodo origen especificado; estos nodos se almacenan en el conjunto T. En el paso $(k + 1)$ se añade a la lista T aquel nodo que presente el camino más corto desde el nodo origen y que no se encuentre ya incluido en dicha lista. A medida que se incorporan nuevos nodos a T, se define su camino desde el origen. El algoritmo se puede describir formalmente como sigue. Definamos:

N = conjunto de nodos de la red.

s = nodo origen.

T = lista o conjunto de nodos añadidos o incorporados por el algoritmo.

$w(i, j)$ = coste del enlace desde el nodo i al nodo j; $w(i, i) = 0$; $w(i, j) = \infty$ si los dos nodos no se encuentran directamente conectados; $w(i, j) \geqslant 0$ si los dos nodos están directamente conectados.

$L(n)$ = coste en curso obtenido por el algoritmo para el camino de mínimo coste del nodo s al nodo n; al finalizar el algoritmo, este coste corresponde al del camino de mínimo coste de s a n en el grafo.

El algoritmo consta de tres pasos, repitiéndose los pasos 2 y 3 hasta que $T = N$; es decir, hasta que las rutas finales han sido asignadas a todos los nodos en la red:

1. **[Inicialización]**

   $T = \{s\}$ El conjunto de nodos incorporados sólo consta del nodo origen s.

   $L(n) = w(s, n)$, para $n \neq s$ El coste inicial de las rutas a los nodos vecinos es el asociado a los enlaces.

2. **[Obtención del siguiente nodo]** Se busca el nodo vecino que no esté en T con el camino de menor coste desde s y se incorpora a T; también se incorporará el enlace desde ese nodo hasta un nodo de T que forma parte del camino. Esto se puede expresar como

   $$\text{Encontrar } x \notin T \text{ tal que } L(x) = \min_{j \notin T} L(j)$$

   Añadir x a T, incorporando también el enlace desde x que contribuye a $L(x)$ como la componente de menor coste (es decir, el último salto en la ruta).

3. **[Actualización de los caminos de mínimo coste]**

   $$L(n) = \min [L(n), L(x) + w(x, n)] \quad \text{para todo } n \notin T$$

Si el último término es el mínimo, el camino desde s hasta n es ahora el camino desde s hasta x concatenado con el enlace desde x hasta n.

El algoritmo concluye cuando todos los nodos han sido añadidos a T. Al final, el valor $L(x)$ asociado a cada nodo x es el coste (longitud) de la ruta de mínimo coste de s a x. Además, T define la ruta de mínimo coste desde s hasta cualquier otro nodo.

Cada iteración de los pasos 2 y 3 incorpora un nuevo nodo a T y define el camino de mínimo coste desde s hasta ese nodo, atravesando dicha ruta sólo nodos incluidos en T. Para comprender mejor esto considérese el siguiente razonamiento. Tras k iteraciones existen k nodos en T, habiéndose obtenido además el camino de mínimo coste desde s hasta cada uno de esos nodos. Consideremos ahora todos los caminos posibles desde s hasta los nodos no incluidos en T. Entre estos caminos existe uno de mínimo coste que pasa exclusivamente a través de nodos en T (*véase* Ejercicio 12.4), terminando con un enlace directo entre algún nodo en T y un nodo no incluido en esta lista. Este nodo se añade a T y se define el camino asociado como la ruta de mínimo coste para ese nodo.

En la Tabla 12.2a y en la Figura 12.10 se muestra el resultado de aplicar el algoritmo al grafo de la Figura 12.2 con $s = 1$. Los enlaces sombreados definen el árbol de expansión correspondiente al grafo, mientras que los valores que aparecen rodeados por un círculo corresponden a la estimación actual de $L(x)$ para cada nodo x. Los nodos sombreados representan la incorporación de éstos a T. Obsérvese que en cada etapa se obtiene el camino a cada nodo, así como el coste total asociado al mismo. Tras la última iteración se dispone del camino de mínimo coste a cada nodo y del coste asociado. El mismo procedimiento se puede utilizar considerando como nodo origen el 2, y así sucesivamente.

ALGORITMO DE BELLMAN-FORD

El algoritmo de Bellman-Ford [FORD62] se puede enunciar así: encontrar los caminos más cortos desde un nodo origen dado con la condición de que éstos contengan a lo sumo un enlace; a continuación encontrar los caminos más cortos con la condición de que contengan dos enlaces como

Tabla 12.2. Ejemplo de algoritmos de encaminamiento de mínimo coste (haciendo uso de la Figura 12.2).

a) Algoritmo de Dijkstra ($s = 1$)

Iteración T		$L(2)$	Ruta	$L(3)$	Ruta	$L(4)$	Ruta	$L(5)$	Ruta	$L(6)$	Ruta
1	{1}	2	1-2	5	1-3	1	1-4	∞	—	∞	—
2	{1, 4}	2	1-2	4	1-4-3	1	1-4	2	1-4-5	∞	—
3	{1, 2, 4}	2	1-2	4	1-4-3	1	1-4	2	1-4-5	∞	—
4	{1, 2, 4, 5}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
5	{1, 2, 3, 4, 5}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
6	{1, 2, 3, 4, 5, 6}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6

b) Algoritmo de Bellman-Ford ($s = 1$)

h	$L_h(2)$	Ruta	$L_h(3)$	Ruta	$L_h(4)$	Ruta	$L_h(5)$	Ruta	$L_h(6)$	Ruta
0	∞	—	∞	—	∞	—	∞	—	∞	—
1	2	1-2	5	1-3	1	1-4	∞	—	∞	—
2	2	1-2	4	1-4-3	1	1-4	2	1-4-5	10	1-3-6
3	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
4	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6

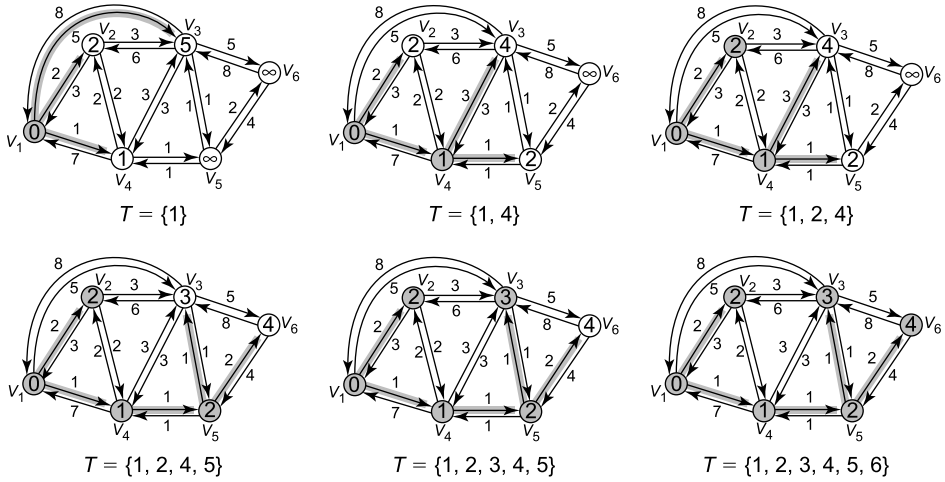


Figura 12.10. Algoritmo de Dijkstra aplicado al grafo de la Figura 12.2.

máximo, y así sucesivamente. Este algoritmo actúa también en pasos, pudiéndose describir formalmente como sigue. Definamos:

s = nodo origen.

$w(i, j)$ = coste del enlace desde el nodo i al nodo j; $w(i, i) = 0$; $w(i, j) = \infty$ si los dos nodos no se encuentran directamente conectados; $w(i, j) \geqslant 0$ si los dos nodos están directamente conectados.

h = número máximo de enlaces en un camino en el paso actual del algoritmo.

$L_h(n)$ = coste del camino de mínimo coste desde el nodo s hasta el nodo n con la condición de que no haya más de h enlaces.

1. [Inicialización]

$$L_0(n) = \infty, \forall\ n \neq s$$
$$L_h(s) = 0, \forall\ h$$

2. [Actualización]

Para cada sucesivo $h \geqslant 0$:

Para cada $n \neq s$, calcular

$$L_{h+1}(n) = \min_j [L_h(j) + w(j, n)]$$

Conectar n con el nodo predecesor j de mínimo coste y eliminar todas las conexiones de n con un nodo predecesor diferente obtenido en una iteración anterior. El camino de s a n finaliza con el enlace de j a n.

Para la iteración del paso 2 con $h = K$, y para cada nodo de destino n, el algoritmo compara las rutas potenciales de longitud $K + 1$ desde s hasta n con el camino existente al final de la iteración anterior. Si el camino más corto previo tiene un coste inferior, se guarda; en caso contrario, se define un nuevo camino de longitud $K + 1$ de s a n, el cual consiste en una ruta de longitud K de s a algún nodo j más un salto directo desde el nodo j hasta el nodo n. En este caso, el camino de s a j considerado corresponde a la ruta de K saltos para j definida en la iteración anterior (*véase* Ejercicio 12.5).

En la Tabla 12.2b y en la Figura 12.11 se muestra el resultado de aplicar este algoritmo a la Figura 12.2 usando $s = 1$. En cada etapa se determinan las rutas de mínimo coste con un número máximo de enlaces igual a h. Tras la última iteración se conoce el camino de mínimo coste a cada nodo y el coste asociado. El mismo procedimiento se puede usar tomando como nodo origen el nodo 2, y así sucesivamente. Obsérvese que los resultados coinciden con los obtenidos por el algoritmo de Dijkstra.

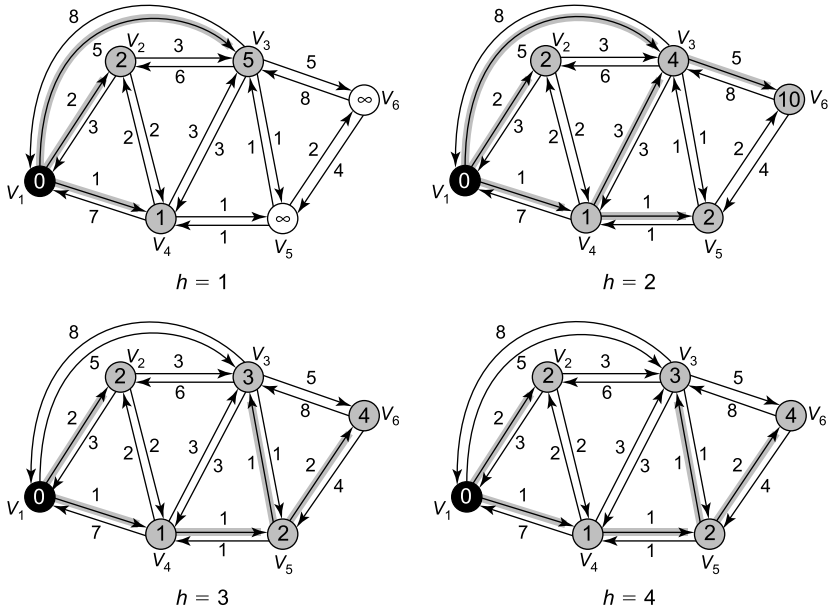


Figura 12.11. Algoritmo de Bellman-Ford aplicado al grafo de la Figura 12.2.

COMPARACIÓN

Una comparación interesante entre estos dos algoritmos hace referencia a la información necesaria a considerar. Veamos en primer lugar el algoritmo de Bellman-Ford. En el paso 2 del proceso, el cálculo para el nodo n requiere conocer el coste de los enlaces a todos los nodos vecinos de n —es decir, $w(j, n)$— además del coste total del camino a cada uno de estos nodos desde un nodo origen particular s —es decir, $L_h(j)$—. Cada nodo puede mantener un conjunto de costes y rutas asociadas para cada uno de los otros nodos en la red e intercambiar periódicamente esta información con sus vecinos directos. Por tanto, cada nodo puede hacer uso de la expresión dada en el paso 2 del algoritmo de Bellman-Ford, basándose sólo en la información dada por sus vecinos y en el conocimiento del coste de las líneas asociadas, para actualizar los caminos y sus costes. Consideremos ahora el algoritmo de Dijkstra. En el paso 3 parece necesitarse que cada nodo disponga de la información completa acerca de la topología de la red; es decir, cada nodo debe conocer todos los enlaces y los costes asociados a ellos. Así, en este algoritmo, la información se debe intercambiar con todos los demás nodos.

En general, en la evaluación de las ventajas relativas de ambos algoritmos se debe considerar el tiempo de procesamiento de los algoritmos y la cantidad de información a obtener del resto de nodos de la red o de la internet, dependiendo dicha evaluación de la implementación específica.

Por último, se ha de reseñar que ambos algoritmos convergen, y lo hacen hacia la misma solución bajo condiciones estáticas de la topología y del coste de los enlaces. Si el coste de los enlaces varía a lo largo del tiempo, el algoritmo tratará de reflejar estos cambios; sin embargo, si el coste de los enlaces depende del tráfico, que a su vez depende de las rutas elegidas, se produce una realimentación que puede provocar una situación de inestabilidad.

12.4. LECTURAS RECOMENDADAS

En [GIRA90] se ofrece un estudio adecuado acerca del encaminamiento en redes de conmutación de circuitos. [CORM01] contiene un análisis detallado de los algoritmos de mínimo coste presentados en el capítulo, discutiéndose también en detalle estos algoritmos en [BERT92].

BERT92 Bertsekas, D. y Gallager, R. *Data Networks*. Upper Saddle River, NJ: Prentice Hall, 1992.

CORM01 Cormen, T., et al., *Introduction to Algorithms*. Cambridge, MA: MIT Press, 2001.

GIRA90 Girard, A. *Routing and Dimensioning in Circuit-switching Networks*. Reading, MA: Addison-Wesley, 1990.

12.5. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

algoritmo de Bellman-Ford
algoritmo de Dijkstra
algoritmos de mínimo coste
encaminamiento adaptable
encaminamiento aleatorio
encaminamiento alternativo
encaminamiento estático
inundaciones

CUESTIONES DE REPASO

12.1. ¿Qué es el tráfico en horas punta?

12.2. ¿Cuál es compromiso más importante en el diseño de un esquema de encaminamiento para redes de conmutación de circuitos?

12.3. ¿Cuáles son las diferencias entre encaminamiento estático y encaminamiento alternativo en redes de conmutación de circuitos?

12.4. ¿Cuáles son los requisitos principales a tener en consideración en la función de encaminamiento en una red de conmutación de paquetes?

12.5. ¿Qué es el encaminamiento estático?

12.6. ¿En qué consiste el esquema de inundaciones?

12.7. ¿Cuáles son las ventajas y desventajas del encaminamiento adaptable?

12.8. ¿Qué es un algoritmo de mínimo coste?

12.9. ¿Cuál es la diferencia principal entre el algoritmo de Dijkstra y el de Bellman-Ford?

EJERCICIOS

12.1. Considere una red de conmutación de paquetes con N nodos conectados formando las siguientes topologías:

a) Estrella: un nodo central sin ninguna estación conectada y con todos los otros nodos conectados a él.

b) Bucle: cada nodo está conectado a otros dos nodos formando un bucle cerrado.

c) Completamente conectada: cada nodo está directamente conectado a todos los otros nodos.

Determine el número medio de saltos entre estaciones en cada caso.

12.2. Considere una red de conmutación de paquetes con topología en árbol binario. El nodo raíz se conecta a otros dos nodos y todos los nodos intermedios se encuentran conectados con un nodo en la dirección hacia el nodo raíz y con dos en la dirección contraria. En la parte inferior existen nodos con un solo enlace hacia el nodo raíz. Si hay $2^N - 1$ nodos, obtenga una expresión para el número medio de saltos por paquete para un valor de N elevado suponiendo que los trayectos entre todos los pares de nodos son aproximadamente iguales. *Sugerencia:* las siguientes igualdades le serán de utilidad:

$$\sum_{i=1}^{\infty} X^i = \frac{X}{1-X} \quad ; \quad \sum_{i=1}^{\infty} iX^i = \frac{X}{(1-X)^2}$$

12.3. Para determinar la ruta de mínimo coste desde un nodo s a un nodo t, el algoritmo de Dijkstra se puede expresar mediante el siguiente programa:

```
for n:=1 to N do
   begin
         L[n]:=∞; final[n]:=false;      {todos los nodos se etiquetan
                                         temporalmente con ∞}
```

```
          pred[n]:=1
    end;
L[s]:=0; final[s]:=true;  {el nodo s se etiqueta permanentemente con 0}
recent:=s;                {el nodo más reciente para ser etiquetado
                           permanentemente es s}

path:=true;
{inicialización}

while final[t]=false do
begin
     for n:=1 to N do  {encontrar nueva etiqueta}
         if (w[recent,n]< ∞) AND (NOT final[n]) then
                        {para cada sucesor inmediato de recent que no se
                          encuentra permanentemente etiquetado, hacer}
              begin {actualizar las etiquetas temporales}
                    newlabel:=L[recent]+w[recent,n];
                    if newlabel<L[n] then
                      begin L[n]:=newlabel; pred[n]:=recent end
                      {se etiqueta de nuevo n si existe un camino
                      más corto a través del nodo recent y se hace
                      recent el predecesor de n en el camino más corto desde s}
              end;
     temp:= ∞;
     for x:=1 to N do  {encontrar el nodo con la etiqueta temporal menor}
          if (NOT final[x]) AND (L[x]<temp) then
               begin y:=x; temp:=L[x] end;
     if temp<∞ then {existe una ruta} then
          begin final[y]:=true; recent:=y end
          {y, el siguiente nodo más cercano a s, se
          etiqueta permanentemente}
     else begin path:=false; final[t]:=true end
end
```

En este programa se le asigna temporalmente una etiqueta inicial a cada nodo. Cuando se obtiene una ruta final a un nodo, se le asigna una etiqueta permanente igual al coste del camino desde *s*. Escriba un programa similar para el algoritmo de Bellman-Ford. *Sugerencia:* el algoritmo de Bellman-Ford se conoce a veces como método de corrección de etiquetas, frente al método de fijado de etiquetas seguido en el algoritmo de Dijkstra.

12.4. En la descripción del algoritmo de Dijkstra dada en la Sección 12.3 se dice que en cada iteración se añade un nuevo nodo a T y que la ruta de mínimo coste para ese nuevo nodo sólo atraviesa nodos ya incluidos en T. Demuestre que esto es cierto. *Sugerencia:* comience por el principio. Muestre que el primer nodo añadido a T debe tener un enlace directo al nodo origen, el segundo nodo en T debe tener un enlace directo con el nodo origen o con el primer nodo incluido en T, y así sucesivamente. Recuerde que los costes de todas las líneas se suponen no negativos.

12.5. En la descripción del algoritmo de Bellman-Ford se establece que en la iteración para la que $h = K$, si hay definida alguna ruta de longitud $K + 1$, los primeros K saltos de este camino forman una ruta definida en la iteración anterior. Demuestre que es cierto.

12.6. Los valores del camino de mínimo coste en el paso 3 del algoritmo de Dijkstra sólo se actualizan para nodos no incluidos aún en *T*. ¿No es posible encontrar una ruta de mínimo coste para un nodo en *T*? Si es así, demuéstrelo con un ejemplo. En caso contrario, justifique razonadamente el motivo.

12.7. Haciendo uso del algoritmo de Dijkstra, genere un camino de mínimo coste para los nodos del 2 al 6 con el resto de nodos de la Figura 12.2. Muestre los resultados como en la Tabla 12.2a.

12.8. Repita el Ejercicio 12.7 haciendo uso del algoritmo de Bellman-Ford.

12.9. Aplique el algoritmo de encaminamiento de Dijkstra para las redes de la Figura 12.12. Obtenga una tabla similar a la Tabla 12.2a y una figura análoga a la Figura 12.10.

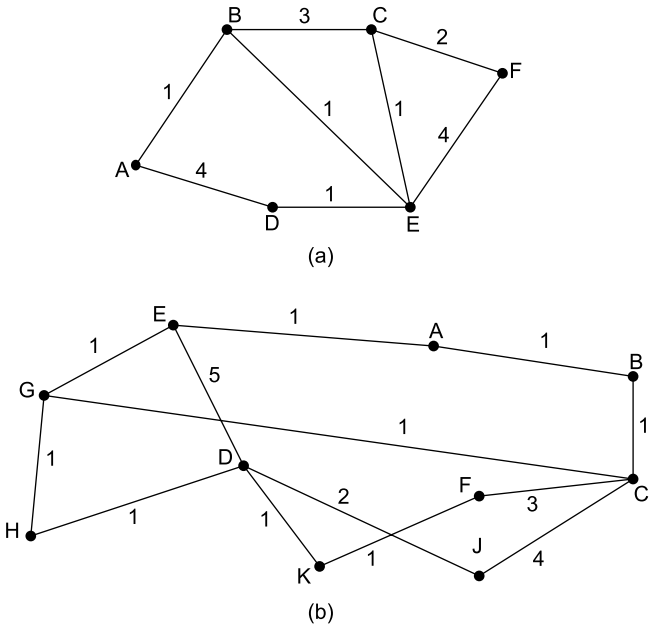


Figura 12.12. Redes de la conmutación de paquetes con costes de enlace asociados.

12.10. Repita el Ejercicio 12.9 haciendo uso del algoritmo de Bellman-Ford.

12.11. ¿Proporcionan los algoritmos de Dijkstra y de Bellman-Ford los mismos resultados siempre? ¿Por qué sí o por qué no?

12.12. Tanto el algoritmo de Dijkstra como el de Bellman-Ford obtienen las rutas de mínimo coste desde un nodo al resto. Por su parte, el algoritmo de Floyd-Warshall obtiene los caminos de mínimo coste entre todos los pares de nodos posibles. Se define:

N = conjunto de nodos en la red.

$w(i, j)$ = coste del enlace del nodo i al nodo j; $w(i, i) = 0$ y $w(i, j) = \infty$ si los dos nodos no se encuentran directamente conectados.

$L_n(i, j)$ = coste del camino de mínimo coste desde el nodo i al nodo j con la condición de que sólo los nodos 1, 2, ..., n se pueden usar como nodos intermedios en las rutas.

El algoritmo sigue los siguientes pasos:

1. Inicialización:

$$L_0(i, j) = w(i, j), \text{ para todo } i, j, i \neq j$$

2. Para $n = 0, 1, ..., N - 1$, $L_{n+1}(i, j) = \min [L_n(i, j), L_n(i, n + 1) + L_n(n + 1, j)]$, $\forall\ i \neq j$ explique el algoritmo con palabras. Demuestre por inducción que funciona correctamente.

12.13. El nodo 1 de la Figura 12.4 envía un paquete al nodo 6 usando inundaciones. Contabilizando la transmisión de un paquete sobre una línea como una carga de uno, indique cuál será el tráfico total generado si:

a) Cada nodo descarta los paquetes entrantes duplicados.

b) Se usa un campo de cuenta de saltos con un valor inicial igual a 5 y no se descartan los paquetes duplicados.

12.14. Ya se vio que el algoritmo de inundaciones se puede utilizar para determinar la ruta con menor número de saltos. ¿Se puede usar también para la obtención del camino con menor retardo?

12.15. El algoritmo de encaminamiento aleatorio sólo permite la existencia de una copia de un paquete en un instante de tiempo dado. A pesar de ello, resulta deseable la utilización de un campo de cuenta de saltos. ¿Por qué?

12.16. Otro esquema de encaminamiento adaptable es el conocido como aprendizaje hacia atrás (*backward learning*). Todo paquete encaminado a través de la red contiene no sólo la dirección de destino, sino también la dirección de origen más un contador de saltos que se incrementa en cada salto. Cada nodo construye una tabla de encaminamiento que especifica el nodo siguiente y el número de saltos para cada destino. ¿Cómo se usa la información contenida en el paquete para construir la tabla? ¿Cuáles son las ventajas y desventajas de esta técnica?

12.17. Construya una tabla de encaminamiento centralizado para las redes de la Figura 12.12.

12.18. Considérese un sistema que emplea la técnica de inundaciones con un contador de saltos que se supone inicialmente igual al «diámetro» de la red. Cuando el contador alcanza el valor cero el paquete se descarta, excepto en el destino. ¿Se asegura siempre así que el paquete alcanzará el destino si existe al menos un camino operativo? Justifique la respuesta.

CAPÍTULO 13

Congestión en redes de datos

13.1. Efectos de la congestión
Funcionamiento ideal
Funcionamiento real

13.2. Control de congestión
Contrapresión
Paquetes de obstrucción
Señalización implícita de congestión
Señalización explícita de congestión

13.3. Gestión de tráfico
Imparcialidad
Calidad de servicio
Reservas

13.4. Control de congestión en redes de conmutación de paquetes

13.5. Control de congestión en retransmisión de tramas
Gestión de la tasa de tráfico
Prevención de congestión mediante señalización explícita

13.6. Gestión de tráfico en ATM
Requisitos para el control de tráfico y de congestión en ATM
Efectos de latencia/velocidad
Variación del retardo de celdas
Control de tráfico y de congestión
Técnicas de gestión de tráfico y de control de congestión

13.7. Gestión de tráfico GFR en ATM
Mecanismos de soporte de tasas garantizadas
Definición de adecuación GFR
Mecanismo para la comprobación de elegibilidad de QoS

13.8. Lecturas recomendadas

13.9. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- El problema de la congestión se produce cuando el número de paquetes que se transmite a través de una red comienza a aproximarse al límite de la capacidad de gestión de paquetes de la misma. El objetivo del control de congestión es mantener el número de paquetes en la red por debajo del nivel para el que decaen dramáticamente las prestaciones.
- La ausencia de mecanismos de control de flujo en los protocolos ATM y de retransmisión de tramas dificulta el control de congestión. Se han desarrollado diversas técnicas para hacer frente a la congestión y garantizar distintas calidades de servicio para diferentes tipos de tráfico.
- En las redes ATM se lleva a cabo un acuerdo de tráfico con cada usuario que especifica las características del tráfico esperado y del tipo de servicio a proveer por la red. La red implementa técnicas de control de congestión para proteger a ésta de la congestión, al tiempo que se cumplen los acuerdos de tráfico establecidos.
- Una red ATM supervisa el flujo de celdas procedente de cada fuente y puede rechazar o marcar para su rechazo potencial aquellas celdas que excedan los acuerdos de tráfico establecidos. Además, la red puede adaptar el tráfico procedente de los usuarios y suavizar los flujos de tráfico de salida mediante el almacenamiento temporal de las celdas.

El control de congestión es un aspecto de diseño de consideración necesario en las redes de datos, como las de conmutación de paquetes, las de retransmisión de tramas y las redes ATM, y en la interconexión de redes (internet). El control de la congestión, como el fenómeno de la propia congestión en sí, es un problema complejo. En términos muy generales, la congestión ocurre cuando el número de paquetes[1] que se transmiten sobre una red comienza a aproximarse al límite de la capacidad de gestión de paquetes de la misma. El objetivo del control de congestión es mantener el número de paquetes en la red por debajo del nivel para el que decaen dramáticamente las prestaciones.

Para comprender los elementos involucrados en el control de la congestión hemos de fijarnos en algunos resultados de la teoría de colas. Una red de datos o una internet es, esencialmente, una red de colas, de modo que en cada nodo (un conmutador en una red de datos, un dispositivo de encaminamiento en una internet) existe una cola de paquetes asociada a cada canal de salida. Si la velocidad a la que se reciben y ponen en cola los paquetes supera la velocidad a la que éstos se pueden transmitir, el tamaño de la cola crece sin límite y el retardo sufrido por los paquetes tiende a infinito. Incluso si la velocidad de llegada de los paquetes es menor que la de transmisión de éstos, el tamaño de la cola crecerá drásticamente conforme la primera se aproxime a la segunda. Como regla empírica, cuando el porcentaje de utilización de la línea en la que se ponen en cola los paquetes supera el 80 por ciento, el tamaño de la cola crece de forma alarmante. Este crecimiento del tamaño de la cola implica el aumento del retardo sufrido por un paquete en cada nodo. Así pues, dado que el tamaño de una cola cualquiera es finito, cuando éste crece se producirá el desbordamiento de la cola.

[1] En este capítulo se usa el término *paquete* en un sentido muy amplio para hacer referencia a paquetes en una red de conmutación de paquetes, a tramas en una red de retransmisión de tramas, a celdas en una red ATM o a datagramas IP en una internet.

Este capítulo se centra en el control de congestión en redes de datos conmutadas, incluyendo redes de conmutación de paquetes, de retransmisión de tramas y ATM. Los principios que se examinan son igualmente aplicables a la interconexión de redes (Internet). En la Parte V del texto se estudiarán mecanismos de control de congestión adicionales en la discusión sobre la operación de la interconexión de redes y el control de congestión en TCP.

13.1. EFECTOS DE LA CONGESTIÓN

Considérese la situación de las colas en un nodo de conmutación de paquetes o en un dispositivo de encaminamiento como se muestra en la Figura 13.1. Todos los nodos tienen un número de puertos de entrada/salida[2] conectados: uno o más hacia otros nodos y cero o más hacia sistemas finales. Los paquetes se reciben y transmiten por cada puerto. Consideremos la existencia de dos memorias temporales, o colas, para cada puerto, una para aceptar los paquetes de llegada y otra para gestionar los paquetes a transmitir. En la práctica, podrían existir dos memorias temporales de tamaño fijo asociadas a cada uno de los puertos, o bien una única memoria para todas las actividades de almacenamiento. El último caso es equivalente a pensar que cada puerto dispone de dos memorias temporales de tamaño variable con la restricción de que la suma de todas ellas es constante.

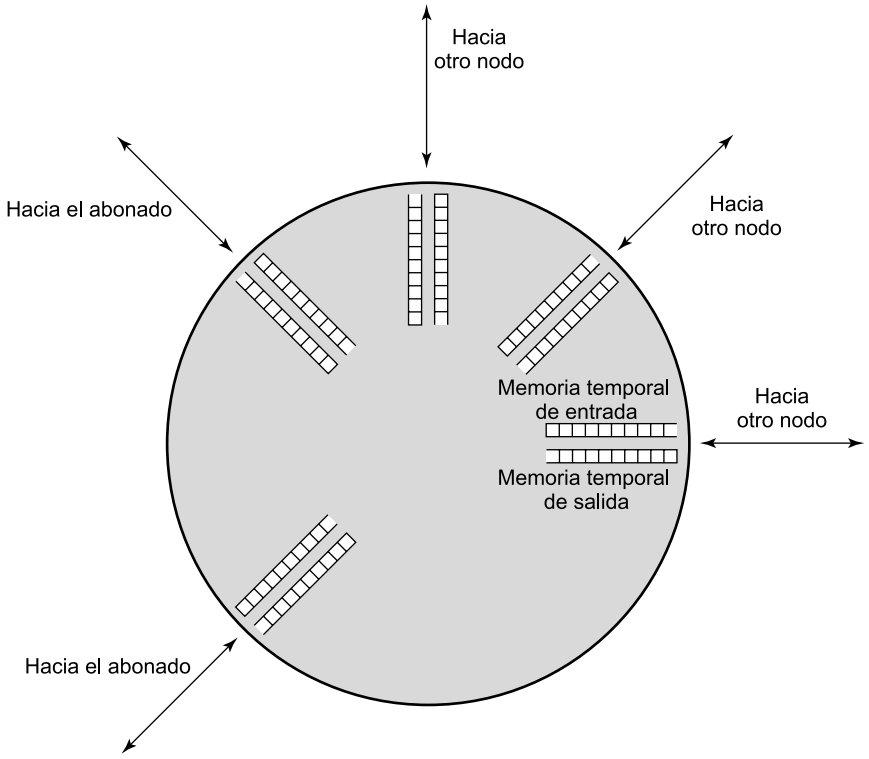


Figura 13.1. Colas de entrada y salida de un nodo.

[2] En el caso de un nodo de conmutación en una red de conmutación de paquetes, de retransmisión de tramas o ATM, cada puerto de entrada/salida conecta con una línea de transmisión a otro nodo o sistema final. En el caso de un dispositivo de encaminamiento en una red Internet, cada puerto de entrada/salida conecta con un enlace directo a otro nodo o con una subred.

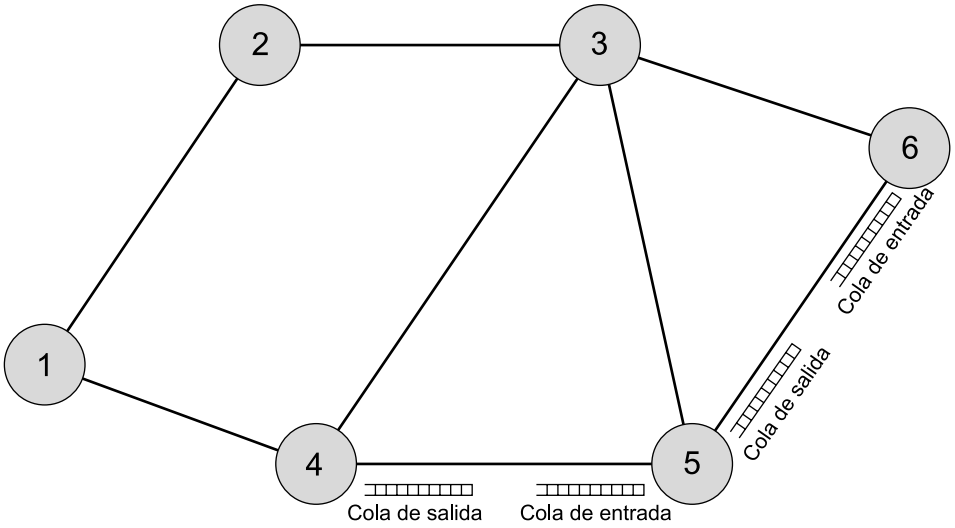


Figura 13.2. Interacción de las colas en una red de datos.

En cualquier caso, a medida que se reciben los paquetes, se almacenan en la memoria temporal de entrada del puerto correspondiente. El nodo examina cada paquete de entrada para tomar una decisión de encaminamiento y lo coloca en la memoria temporal de salida pertinente. Los paquetes en cola se transmiten tan rápido como es posible, lo que corresponde a multiplexación por división en el tiempo estadística. Si los paquetes se reciben en el nodo demasiado deprisa para ser procesados (toma de decisión de encaminamiento), o más rápido de lo que requiere el borrado de los paquetes en la memoria temporal de salida, no existirá eventualmente memoria temporal disponible para los paquetes recibidos.

Cuando se alcanza este punto de saturación, se pueden adoptar dos estrategias. La primera consiste simplemente en descartar cualquier paquete de entrada para el que no exista memoria disponible. La alternativa es que el nodo que sufra este problema implemente algún tipo de control de flujo sobre sus vecinos de forma que el tráfico sea manejable. El problema es que, como se ilustra en la Figura 13.2, cada uno de los nodos vecinos gestiona también varias colas. Así, si el nodo 6 frena el flujo de paquetes del nodo 5, se llenará la memoria temporal de salida del nodo 5 asociada al puerto hacia 6. De esta manera, la congestión sufrida en un punto de la red se propagará rápidamente a otra zona o incluso a toda la red. Aunque el control de flujo es una herramienta muy potente, debe utilizarse de forma que se gestione el tráfico de toda la red.

FUNCIONAMIENTO IDEAL

En la Figura 13.3 se muestra el comportamiento ideal de la utilización de una red. La gráfica superior representa el rendimiento de la red (número de paquetes enviados a sistemas finales destino) en función de la carga ofrecida (número de paquetes transmitidos por sistemas finales origen), ambos parámetros normalizados al rendimiento máximo teórico de la red. Por ejemplo, si una red consta de un único nodo con dos líneas *full-duplex* a 1 Mbps, la capacidad teórica de la red será 2 Mbps, correspondiendo a un flujo de 1 Mbps en cada sentido. En el caso ideal, el rendimiento de la red crece hasta aceptar una carga igual a la capacidad total de la red, permaneciendo el rendimiento normalizado a valor 1.0 para cargas de entrada superiores. Obsérvese, sin embargo, lo que sucede con el retardo extremo a extremo medio experimentado por un paquete, incluso bajo esta

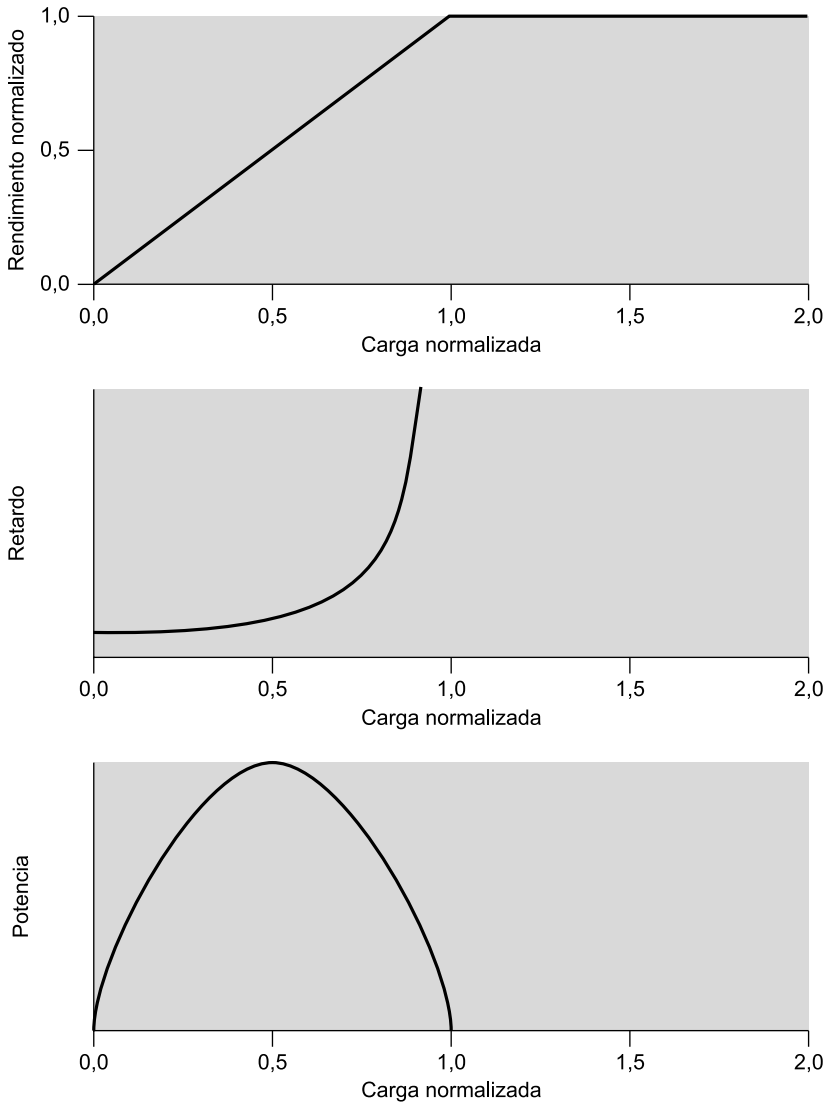


Figura 13.3. Utilización ideal de una red.

suposición de funcionamiento ideal. Cuando la carga es despreciable, existe un retardo pequeño constante consistente en el retardo de propagación a través de la red desde el origen hasta el destino más un retardo de procesamiento en cada nodo. A medida que la carga de la red aumenta, al valor de retardo fijo anterior se suman los retardos de las colas en cada nodo. Finalmente, cuando la carga excede la capacidad de la red, el retardo aumenta sin límite.

Existe una sencilla explicación intuitiva sobre por qué el retardo tiende a infinito. Supongamos que cada nodo de la red dispone de memorias temporales de tamaño infinito y que la carga de entrada supera la capacidad de la red. Bajo condiciones ideales, la red continuará presentando un rendimiento normalizado de 1.0, por lo que la velocidad de salida de paquetes de la red será 1.0. Dado que la velocidad de entrada de paquetes a la red es mayor que 1.0, el tamaño de las colas internas crece. En el estado estacionario, en el que la entrada es superior a la salida, estos

tamaños de cola crecen sin límite y, en consecuencia, los retardos de cola también crecerán de forma ilimitada.

Es importante comprender el significado de la Figura 13.3 antes de pasar a estudiar las condiciones de funcionamiento real. La figura representa el objetivo ideal, inasequible, de todos los esquemas de control de tráfico y de congestión. En ningún esquema se pueden exceder las prestaciones indicadas en la Figura 13.3.

Veremos que el término *potencia* se emplea a veces en la bibliografía existente acerca de las prestaciones de las redes. Este parámetro se define como la relación entre el rendimiento y el retardo, representándose en la gráfica inferior de la Figura 13.3 para el caso ideal. Ya se ha visto que, generalmente, los esquemas de control de configuración y de congestión de red que mejoran el rendimiento presentan también un mayor retardo [JAIN91], y que la potencia es una métrica concisa que puede ser usada para comparar diferentes esquemas.

FUNCIONAMIENTO REAL

En el caso ideal ilustrado en la Figura 13.3 se ha supuesto que las memorias temporales son infinitas y que no existe coste asociado a la transmisión de los paquetes ni al control de congestión. En la práctica, las memorias son finitas, lo que provoca desbordamientos, y el control de congestión consume capacidad de la red debido al intercambio de señales de control.

Considérese lo que sucede en una red con memorias temporales finitas si no se lleva a cabo el control de congestión ni se controla la entrada procedente de los sistemas finales. Aunque es claro que los detalles diferirán según la configuración de la red y las estadísticas de tráfico, obsérvese el descorazonador resultado mostrado en términos generales en la Figura 13.4.

Para baja carga, el rendimiento, y por tanto la utilización de la red, aumenta conforme lo hace la carga. A medida que ésta continúa creciendo, llega un momento (punto A en la gráfica) a partir del cual el rendimiento de la red crece a una velocidad menor a la que lo hace la carga. Este hecho se debe a que la red entra en un estado de congestión moderada, en la cual la red sigue dando curso al tráfico aunque con un incremento en el retardo. El alejamiento del rendimiento de su comportamiento ideal está motivado por varios factores. Por una parte, es improbable la distribución uniforme de la carga a través de la red, de modo que algunos nodos sufrirán una congestión moderada mientras que otros experimentarán una congestión severa y precisarán descartar algún tráfico. Adicionalmente, la red tratará de equilibrar la carga conforme ésta aumenta mediante el encaminamiento de paquetes a través de zonas menos congestionadas. Por lo que se refiere a la función de encaminamiento de la red, los nodos deben intercambiar entre sí un mayor número de paquetes para avisarse acerca de las zonas congestionadas; este coste reduce la capacidad disponible para los paquetes de datos.

A medida que la carga de la red continúa aumentando, el tamaño de las colas de los distintos nodos sigue creciendo. Eventualmente, llega un momento (punto B en la gráfica) a partir del cual el rendimiento real decae al aumentar la carga de entrada. La razón para ello es que las memorias temporales existentes en cada nodo son de tamaño finito. Cuando las memorias en un nodo dado se llenan, éste debe descartar paquetes. Por tanto, los sistemas origen deben retransmitir los paquetes descartados además de otros nuevos. Esto sólo consigue empeorar la situación: conforme se retransmiten más y más paquetes, la carga del sistema aumenta y se saturarán más memorias temporales. Mientras el sistema trata desesperadamente de eliminar el exceso de paquetes, los usuarios continúan enviando paquetes, nuevos y previos, al sistema. Incluso puede que tengan que retransmitirse aquellos paquetes enviados con éxito debido a que una capa superior (por ejemplo, la de

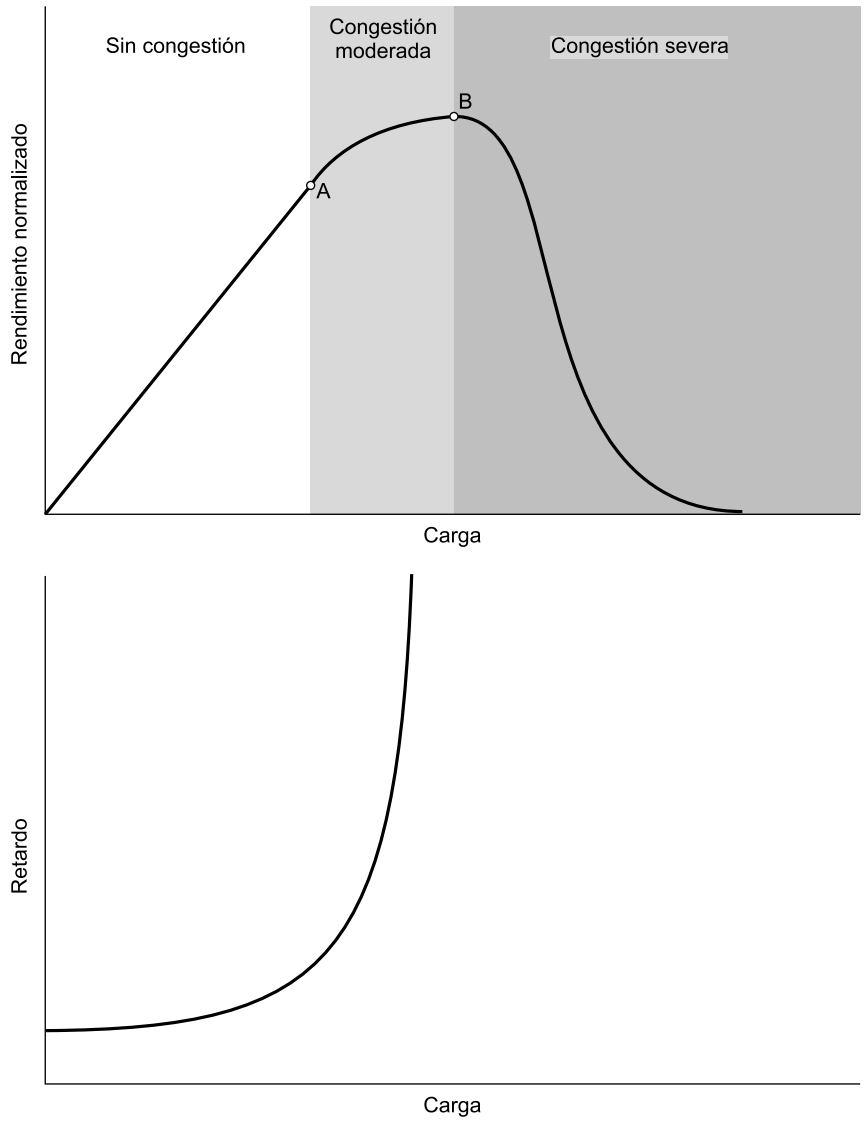


Figura 13.4. Efectos de la congestión.

transporte) tarda mucho tiempo en confirmarlos, por lo que el emisor supone que el paquete no se recibió en el receptor y lo retransmite. En estas circunstancias la capacidad efectiva del sistema decae a cero.

13.2. CONTROL DE CONGESTIÓN

En este libro se presentan distintas técnicas de control de congestión usadas en redes de conmutación de paquetes, de retransmisión de tramas y ATM y en interconexiones de redes basadas en IP. Para situar en su contexto este estudio, la Figura 13.5 muestra un esquema general de las principales técnicas de control de congestión.

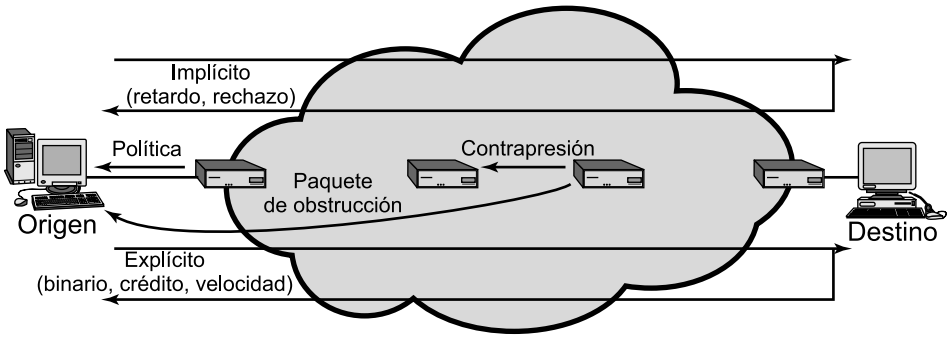


Figura 13.5. Mecanismos para el control de congestión.

CONTRAPRESIÓN

Ya se ha hecho referencia a la contrapresión como técnica de control de congestión. Esta técnica produce un efecto similar a la contrapresión en fluidos que caen por un tubo. Cuando el extremo del tubo está cerrado (u obstruido) el fluido realiza una presión hacia atrás en el tubo hasta el punto de origen, donde el flujo es detenido (o frenado).

La contrapresión se puede realizar a nivel de enlaces o de conexiones lógicas (por ejemplo, circuitos virtuales). Volviendo de nuevo a la Figura 13.2, si el nodo 6 sufre congestión (se llenan las memorias temporales asociadas), éste puede frenar parcial o totalmente el flujo de paquetes desde el nodo 5 (o del nodo 3, o de los dos). Si persiste esta restricción, el nodo 5 necesitará frenar también parcial o totalmente el tráfico sobre sus líneas de entrada. Esta restricción sobre el flujo se propagará hacia atrás (en sentido contrario al flujo del tráfico de datos) hacia los sistemas emisores, cuya transmisión de nuevos paquetes hacia la red quedará limitada.

La contrapresión se puede aplicar de forma selectiva a las conexiones lógicas, de manera que el flujo desde un nodo al siguiente sólo se reduzca o se pare para algunas conexiones, generalmente para aquellas con mayor tráfico. En este caso, la restricción se propagará hacia atrás hacia los emisores a lo largo de las conexiones en cuestión.

La contrapresión resulta de una utilidad limitada, pudiéndose utilizar en redes orientadas a conexión que permiten control de flujo a nivel de enlace (de un nodo al siguiente). Las redes de conmutación de paquetes X.25 presentan generalmente esta característica, pero no así las redes de retransmisión de tramas ni las redes ATM. Por otro lado, las redes IP han sido tradicionalmente construidas de forma que no implementan ningún mecanismo para la regulación del flujo de datos entre dos dispositivos de encaminamiento a lo largo de una ruta a través de la red. No obstante, y como se presentará en la Parte V del libro, recientemente se han desarrollado algunos esquemas basados en flujo relativos a este punto.

PAQUETES DE OBSTRUCCIÓN

Un paquete de obstrucción es un paquete de control generado por un nodo congestionado y transmitido hacia atrás hacia un nodo origen a fin de reducir el flujo de tráfico. Un ejemplo de paquete de obstrucción es el paquete «ralentización del emisor» (*Source Quench*) usado en ICMP (*Internet Control Message Protocol*, protocolo de mensajes de control de Internet). Tanto un dispositivo de encaminamiento como un sistema final destino pueden llevar a cabo el envío de este mensaje hacia

un sistema final origen solicitando la reducción de la velocidad a la que éste emite tráfico hacia la internet de destino. Cuando se recibe un mensaje de ralentización del origen, el sistema emisor reduce la velocidad a la que envía tráfico hacia el destino correspondiente hasta que no reciba más mensajes de ralentización del emisor. Este mensaje se puede usar por parte de un dispositivo de encaminamiento o de un sistema final que debe descartar datagramas IP debido al llenado de una memoria temporal, en cuyo caso el dispositivo de encaminamiento o sistema final generará un mensaje de ralentización del emisor para cada uno de los datagramas que rechaza. Adicionalmente, un sistema se puede anticipar a la ocurrencia de congestión mediante la generación de mensajes de ralentización del emisor cuando la ocupación de sus memorias temporales se aproxime a su capacidad. En este caso, se puede llevar a cabo sin problema la transmisión del datagrama a que hace referencia el mensaje de ralentización del emisor. Por tanto, la recepción de este mensaje no implica el envío o no del datagrama correspondiente.

El uso de paquetes de obstrucción es una técnica relativamente burda para controlar la congestión, presentándose más adelante algunos métodos más sofisticados de señalización explícita de congestión.

SEÑALIZACIÓN IMPLÍCITA DE CONGESTIÓN

Cuando se produce congestión en la red pueden suceder dos cosas: (1) el retardo de transmisión de un paquete dado desde un emisor hasta un destino aumenta hasta ser apreciablemente mayor que el término de retardo de propagación fijo, y (2) se rechazan paquetes. Si un emisor es capaz de detectar el incremento en los retardos y el rechazo de paquetes, tiene una evidencia implícita de la congestión de la red. Si todos los emisores pueden detectar la ocurrencia de congestión y, en respuesta a ella, reducir el flujo, dicha congestión se podrá aliviar. Así pues, el control de congestión en base a la señalización implícita es responsabilidad de los sistemas finales y no precisa acción alguna por parte de los nodos de la red.

La señalización implícita es una técnica de control de congestión efectiva para configuraciones no orientadas a conexión, o datagrama, como redes de conmutación de paquetes mediante datagramas y redes IP. En estos casos, aunque no existen conexiones lógicas a través de la internet sobre las que se pueda regular el tráfico, se pueden establecer conexiones lógicas entre dos sistemas finales a nivel TCP. TCP incluye mecanismos para confirmar la recepción de segmentos TCP y regular el flujo de datos entre el origen y el destino de una conexión TCP. En el Capítulo 20 se estudiarán las técnicas de control de congestión en TCP, basadas en la capacidad de detectar el incremento en el retardo y en la pérdida de segmentos.

La señalización implícita se puede usar también en redes orientadas a conexión. Por ejemplo, en redes de retransmisión de tramas, el protocolo de control LAPF, que es extremo a extremo, incluye funcionalidades similares a las de TCP para el control de flujo y de errores. LAPF de control es capaz de detectar tramas perdidas y adaptar el flujo de datos en consecuencia.

SEÑALIZACIÓN EXPLÍCITA DE CONGESTIÓN

Resulta deseable hacer tanto uso como sea posible de la capacidad disponible de una red, pero manteniendo la capacidad de reaccionar de forma controlada y adecuada ante la congestión. Éste es el objetivo de las técnicas de prevención explícita de congestión. En términos generales, para evitar explícitamente la congestión, la red alerta a los sistemas finales acerca del incremento de la congestión en la red y éstos toman las medidas oportunas para reducir la carga de entrada a la red.

Generalmente, las técnicas explícitas de control de congestión operan sobre redes orientadas a conexión y controlan el flujo de paquetes de conexiones individuales. Las aproximaciones de señalización explícita de congestión pueden trabajar en uno de los dos siguientes sentidos:

- **Hacia atrás:** se notifica al origen que los procedimientos de prevención de congestión deberían ser iniciados allá donde son aplicables para el tráfico en el sentido opuesto al que se recibe la notificación. Se indica así que los paquetes transmitidos por el usuario sobre esta conexión lógica pueden encontrar recursos congestionados. La información hacia atrás se transmite alterando bits en la cabecera de un paquete de datos encabezado por la dirección del emisor a controlar o transmitiendo hacia el origen paquetes de control diferentes de los de datos.
- **Hacia adelante:** se notifica al usuario que los procedimientos de prevención de congestión deberían ser puestos en marcha allá donde son aplicables para el tráfico en el mismo sentido en que se recibe la notificación. Se indica que un paquete dado, sobre una conexión lógica dada, ha encontrado recursos congestionados. De nuevo, esta información se puede transmitir como bits alterados en paquetes de datos o mediante paquetes de control separados. En algunos esquemas, cuando se recibe la señal de notificación hacia adelante en un sistema final, éste devuelve un eco de ella sobre la conexión lógica hacia el emisor. Por su parte, en otros esquemas, se espera que el sistema final realice un control de flujo sobre el sistema final origen en una capa superior (por ejemplo, TCP).

Las técnicas de señalización explícita de congestión se pueden dividir en tres categorías generales:

- **Binarias:** se activa un bit en un paquete de datos transmitido por un nodo congestionado, de modo que un emisor puede reducir su flujo de tráfico cuando recibe una indicación binaria de congestión sobre una conexión lógica.
- **Basadas en crédito:** estos esquemas proporcionan de forma explícita un crédito a un emisor sobre una conexión lógica. Este crédito indica cuántos octetos o cuántos paquetes puede transmitir el emisor, de manera que cuando el crédito se agota el emisor debe esperar la concesión de crédito adicional antes de llevar a cabo el envío de más datos. Los esquemas basados en crédito son usuales para el control de flujo extremo a extremo, en el que un sistema destino hace uso de crédito para evitar que el emisor provoque el desbordamiento de las memorias temporales de recepción, así como para llevar a cabo el control de congestión.
- **Basadas en velocidad:** estos esquemas proporcionan un límite explícito de velocidad para el emisor sobre una conexión lógica, de forma que el origen sólo puede transmitir datos por debajo de este límite. Para controlar la congestión, cualquier nodo a lo largo del camino de la conexión puede reducir el límite de la velocidad mediante el envío de un mensaje de control hacia el emisor.

13.3. GESTIÓN DE TRÁFICO

Existen numerosas cuestiones relacionadas con el control de congestión que podrían incluirse bajo el título general de gestión de tráfico. En su forma más simple, el control de congestión está relacionado con el uso eficiente de una red con alta carga. Cuando se presenta una situación así, se pueden aplicar los distintos mecanismos estudiados en la sección anterior, sin importar el emisor o el destino particulares afectados. Cuando un nodo se satura y debe rechazar paquetes se puede aplicar alguna regla sencilla como la consistente en el rechazo de los paquetes más recientemente

recibidos. Sin embargo, se pueden utilizar otras consideraciones para mejorar la aplicación de las técnicas de control de congestión y de la política de rechazo. A continuación, se presentan brevemente varios de estos criterios.

IMPARCIALIDAD

A medida que aumenta la congestión, los flujos de paquetes entre los emisores y los destinos sufrirán aumentos en el retardo y, para alta congestión, pérdidas de paquetes. Sería deseable asegurar que, como mínimo, los distintos flujos sufran congestión en la misma medida. El simple hecho de rechazar paquetes de acuerdo con la regla último-recibido-primero-descartado puede no resultar justo. Un ejemplo de una técnica que podría ser adecuada consiste en el mantenimiento por parte de los nodos de una cola separada para cada conexión lógica o para cada pareja origen-destino. Si todas las memorias temporales asociadas a las colas tienen el mismo tamaño, las colas con mayor tráfico sufrirán rechazos más a menudo, permitiendo que las conexiones con bajo tráfico compartan la capacidad.

CALIDAD DE SERVICIO

Se podría desear dar un trato diferente a los distintos flujos de tráfico. Por ejemplo, como se indica en [JAIN92], algunas aplicaciones como voz y vídeo, son sensibles al retardo pero insensibles a la pérdida de datos; otras, como la transferencia de ficheros y el correo electrónico, son insensibles al retardo pero sensibles a las pérdidas; otras más, como los gráficos interactivos o aplicaciones de cómputo interactivo, son sensibles tanto al retardo como a las pérdidas. Por otra parte, hay que señalar que flujos de tráfico distintos tienen prioridades diferentes; por ejemplo, el tráfico de gestión de red, en particular durante la ocurrencia de congestión o fallos, es más importante que el tráfico de aplicación.

Es especialmente importante que durante los periodos de congestión los flujos de tráfico con distintos requisitos sean tratados de forma diferente y se les asigne una calidad de servicio (QoS, *Quality of Service*) diferente. Por ejemplo, un nodo puede transmitir en la misma cola paquetes de alta prioridad con preferencia sobre paquetes con prioridad menor; o un nodo puede mantener diferentes colas con distintos niveles QoS y dar prioridad a los niveles superiores.

RESERVAS

Una forma de evitar la congestión y asegurar al mismo tiempo un servicio de una calidad dada para aplicaciones es el uso de un esquema de reserva. Un esquema de este tipo es una parte integral de las redes ATM. Cuando se establece una conexión lógica, la red y el usuario llevan a cabo un acuerdo de tráfico en el que especifica una velocidad de transmisión, además de otras características del flujo de tráfico. La red acuerda proporcionar una QoS particular mientras el tráfico se encuentre dentro de los parámetros acordados, descartándose o gestionándose según el criterio de mínimo esfuerzo, además de ser susceptible a rechazo, aquel tráfico que exceda estos parámetros. Las reservas a realizar son denegadas si los recursos de la red resultan inadecuados para satisfacerlas. Un tipo de esquema similar ha sido desarrollado para redes IP (RSVP, discutido en el Capítulo 19).

Un aspecto importante del esquema de reservas es el que hace referencia a la política de tráfico (*véase* Figura 13.5). Un nodo de la red, generalmente el nodo al que se encuentra conectado el

sistema final, supervisa el flujo de tráfico y lo compara con el acuerdo realizado, de forma que el exceso de tráfico se descarta o se marca para indicar que es susceptible de ser rechazado o de sufrir retardo.

13.4. CONTROL DE CONGESTIÓN EN REDES DE CONMUTACIÓN DE PAQUETES

Se han propuesto y experimentado un gran número de mecanismos de control de congestión en redes de conmutación de paquetes. Los siguientes son algunos ejemplos:

1. Envío de un paquete de control desde un nodo congestionado hacia todos o algunos nodos emisores. Este paquete de obstrucción frenará total o parcialmente la velocidad de transmisión de los emisores, limitando así el número total de paquetes en la red. Esta aproximación requiere tráfico adicional en la red mientras dure la congestión.
2. Consideración de la información de encaminamiento. Algunos algoritmos de encaminamiento, como los de ARPANET, informan a otros nodos acerca del retardo de un enlace, lo que influye en las decisiones de encaminamiento. Esta información se puede usar también para actuar sobre la velocidad de generación de nuevos paquetes. Dado que estos retardos se encuentran influenciados por las decisiones de encaminamiento, pueden cambiar tan rápidamente que no puedan usarse de forma efectiva en el control de la congestión.
3. Uso de paquetes de sondeo extremo a extremo. Estos paquetes pueden llevar un sello de tiempo para determinar el retardo entre dos extremos particulares. Presenta el inconveniente de introducir datos suplementarios en la red.
4. Permitir a los nodos de conmutación añadir información de congestión a los paquetes que los atraviesan. Existen dos aproximaciones posibles. En la primera, un nodo puede añadir esta información a los paquetes que vayan en dirección contraria a la de la congestión; esta información alcanzará rápidamente el nodo origen, el cual puede reducir el flujo de paquetes en la red. Alternativamente, esta información podría añadirse a los paquetes en la misma dirección de la congestión, en cuyo caso el destino requiere del nodo origen un ajuste de la carga o bien devuelve a éste una señal en los paquetes (o confirmaciones) en dirección opuesta.

13.5. CONTROL DE CONGESTIÓN EN RETRANSMISIÓN DE TRAMAS

El documento I.370 define los siguientes objetivos del control de congestión en retransmisión de tramas:

- Minimización del rechazo de celdas.
- Mantenimiento, con alta probabilidad y mínima varianza, de una calidad de servicio acordada.
- Minimización de la posibilidad de que un usuario final pueda monopolizar los recursos de la red a expensas de otros usuarios finales.
- Sencillez de implementación y de poco coste adicional tanto desde el punto de vista del usuario final como desde el de la red.
- Generación de mínimo tráfico de red adicional.
- Distribución adecuada de los recursos de red entre los usuarios finales.

- Limitación en la expansión de la congestión hacia otras redes y elementos de la red.
- Funcionamiento efectivo independientemente del flujo de tráfico en ambos sentidos entre los usuarios finales.
- Mínima interacción o impacto en otros sistemas en la red de retransmisión de tramas.
- Minimización de la varianza de la calidad del servicio suministrado a conexiones de retransmisión de tramas individuales durante la congestión (por ejemplo, las conexiones lógicas individuales no deberían experimentar una degradación brusca cuando se avecina la congestión o ésta ya se ha producido).

El control de congestión resulta difícil en redes de retransmisión de tramas debido a la limitación de herramientas disponibles en los gestores de tramas (nodos de conmutación de tramas). Se ha mejorado el protocolo de retransmisión de tramas con objeto de maximizar el rendimiento y la eficiencia. Una consecuencia de este hecho es que el gestor de tramas no puede controlar el flujo de tramas de un suscriptor o un gestor de tramas adyacente usando el protocolo de control de flujo de ventana deslizante típico, como el empleado en HDLC.

El control de congestión es responsabilidad conjunta de la red y de los usuarios finales. La red (esto es, el conjunto de gestores de tramas) es el mejor lugar para llevar a cabo la supervisión del grado de congestión, mientras que los usuarios finales constituyen el mejor punto para el control de la congestión mediante la limitación del flujo de tráfico.

En la Tabla 13.1 se enumeran las técnicas de control de congestión definidas en los diversos documentos de ITU-T y ANSI. La **estrategia de rechazo** es la respuesta más básica ante la congestión: cuando ésta llega a ser severa, la red se ve forzada a rechazar tramas. Sería deseable hacer esto de manera equitativa para todos los usuarios.

Tabla 13.1. Técnicas de control de congestión en retransmisión de tramas.

Técnica	Tipo	Función	Elementos clave
Control de rechazo	Estrategia de rechazo	Proporciona ayuda a la red sobre las tramas a rechazar	bit DE
Notificación explícita de congestión hacia atrás	Prevención de congestión	Proporciona ayuda a los sistemas finales acerca de la congestión en la red	bit BECN o mensaje CLLM
Notificación explícita de congestión hacia delante	Prevención de congestión	Proporciona ayuda a los sistemas finales acerca de la congestión en la red	bit FECN
Notificación implícita de congestión	Recuperación de congestión	Un sistema final infiere la existencia de congestión a partir de la pérdida de tramas	Números de secuencia en las PDU de capas superiores

Los procedimientos de **prevención de congestión** se usan con el fin de minimizar el efecto de la congestión en la red. De este modo, estos procedimientos serían iniciados en o antes del punto A en la Figura 13.4 para prevenir que la congestión alcance el punto B. Cerca del punto A existe poca evidencia para los usuarios finales de que la congestión está aumentando, por lo que debe

existir algún mecanismo de **señalización explícita** de la red que ponga en marcha la prevención de congestión.

Los procedimientos de **recuperación de congestión** se usan para prevenir el colapso de la red ante la ocurrencia de una congestión severa. Estos procedimientos se inician generalmente cuando la red ha comenzado a perder tramas debido a la congestión. Esta pérdida de tramas se indica mediante algún software de capas superiores (por ejemplo, el protocolo de control LAPF o TCP), y sirve como mecanismo de **señalización implícita**. Tal y como se muestra en la Figura 13.4, las técnicas de recuperación de congestión operan en torno al punto B y en la región de congestión severa.

ITU-T y ANSI consideran la prevención de congestión mediante señalización explícita y la recuperación de congestión mediante señalización implícita como métodos complementarios del control de congestión en el servicio de retransmisión de tramas.

GESTIÓN DE LA TASA DE TRÁFICO

Como último recurso, una red de retransmisión de tramas debe descartar tramas para combatir la congestión; no existe forma de evitar este hecho. Dado que los gestores de tramas en la red disponen de una cantidad finita de memoria para la puesta en cola de las tramas (*véase* Figura 13.2), es posible la saturación de una cola, siendo por tanto necesario el rechazo de las tramas más recientes u otras tramas.

La forma más sencilla de combatir la congestión es que la red de retransmisión de tramas rechace tramas arbitrariamente, independientemente del origen de una trama dada. En este caso, la mejor estrategia para cualquier sistema final individual consiste en transmitir tramas tan rápido como sea posible, lo cual, claro está, empeora la congestión.

Para mejorar la reserva de los recursos, el servicio de retransmisión de tramas incluye el concepto de tasa de información contratada (CIR, *Committed Information Rate*). Este parámetro es una velocidad, en bits por segundo, que acuerda la red para dar soporte a una conexión particular en modo de trama. Cualquier dato transmitido a una velocidad superior a la CIR es susceptible de ser rechazado cuando se produce congestión. A pesar del uso de término *contratado*, no existe garantía de que se alcance la CIR, pudiéndose ver forzada la red a proporcionar un servicio menor a la CIR para una conexión dada en caso de congestión extrema. Sin embargo, cuando llega la hora de descartar tramas, la red decidirá eliminar las tramas de aquellas conexiones que excedan su CIR antes de descartar tramas que respeten la CIR contratada.

En teoría, cada nodo de retransmisión de tramas debería gestionar sus recursos de manera que la suma de las CIR de todas las conexiones correspondientes a todos los sistemas finales conectados al nodo no supere la capacidad del mismo. Además, la suma de las CIR no debería superar la velocidad de datos física de la interfaz usuario-red, conocida como tasa o velocidad de acceso. La limitación impuesta por la velocidad de acceso se puede expresar como sigue:

$$\sum_i \text{CIR}_{i,j} \leqslant \text{velocidad acceso}_j \tag{13.1}$$

donde

$\text{CIR}_{i,j}$ = tasa de información contratada para la conexión i del canal j.

$\text{velocidad acceso}_j$ = velocidad de datos del canal de acceso de usuario j, entendiendo por canal un canal TDM de velocidad fija entre el usuario y la red.

La consideración de la capacidad del nodo puede provocar la selección de valores menores para algunas de las CIR.

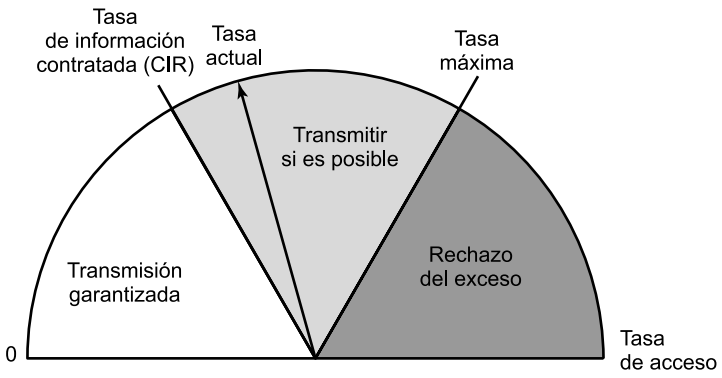


Figura 13.6. Funcionamiento de la CIR.

Para conexiones de retransmisión de tramas permanentes, la CIR de cada conexión se puede establecer en el momento en que se acepta dicha conexión entre el usuario y la red. Para conexiones conmutadas, el parámetro CIR se negocia en la fase de configuración del protocolo de control de llamada.

La CIR provee de un mecanismo de discriminación acerca de qué tramas rechazar cuando se produce congestión. La discriminación se indica mediante el uso del bit de adecuación de rechazo (DE, *Discard Eligibility*) en las tramas LAPF (*véase* Figura 10.19). El gestor de tramas al que se conecta la estación del usuario realiza una función medidora (*véase* Figura 13.6). Si el usuario está enviando datos en una cantidad inferior a la CIR, el gestor de tramas entrantes no altera el bit DE; si, por el contrario, la velocidad excede la CIR, el gestor de tramas entrantes activa el bit DE en las tramas en exceso y las transmite, de modo que estas tramas pueden ser procesadas o, si se produce congestión, rechazadas. Finalmente, se define una velocidad de transmisión máxima de manera que cualquier trama por encima del máximo es descartada cuando llega al gestor de tramas.

La CIR, por sí misma, no proporciona demasiada flexibilidad en la gestión de las tasas de tráfico. En la práctica, un gestor de tramas mide el tráfico sobre cada conexión lógica durante un intervalo de tiempo dado y después toma la decisión en base a la cantidad de datos recibidos durante el intervalo. Son necesarios dos parámetros adicionales, asignados en el caso de conexiones permanentes y negociados para conexiones conmutadas:

- **Tamaño de ráfaga contratado (B_c):** es la máxima cantidad de datos que la red acuerda transmitir, en condiciones normales, en un intervalo de medida T. Estos datos pueden ser o no contiguos (es decir, pueden aparecer en una o en varias tramas).
- **Tamaño de ráfaga en exceso (B_e):** es la máxima cantidad de datos en exceso de B_c que intentará transmitir la red, en condiciones normales, en un intervalo de medida T. Estos datos no se contratan en el sentido de que la red no se compromete a proporcionarlos en condiciones normales. Dicho de otra forma, los datos que representan B_e se envían con menor probabilidad que los datos en B_c.

Las cantidades B_c y CIR están relacionadas. Dado que B_c es la cantidad contratada de datos que puede transmitir el usuario en un tiempo T y CIR es la velocidad a la que se pueden transmitir dichos datos, se tiene que:

$$T = \frac{B_c}{\text{CIR}} \tag{13.2}$$

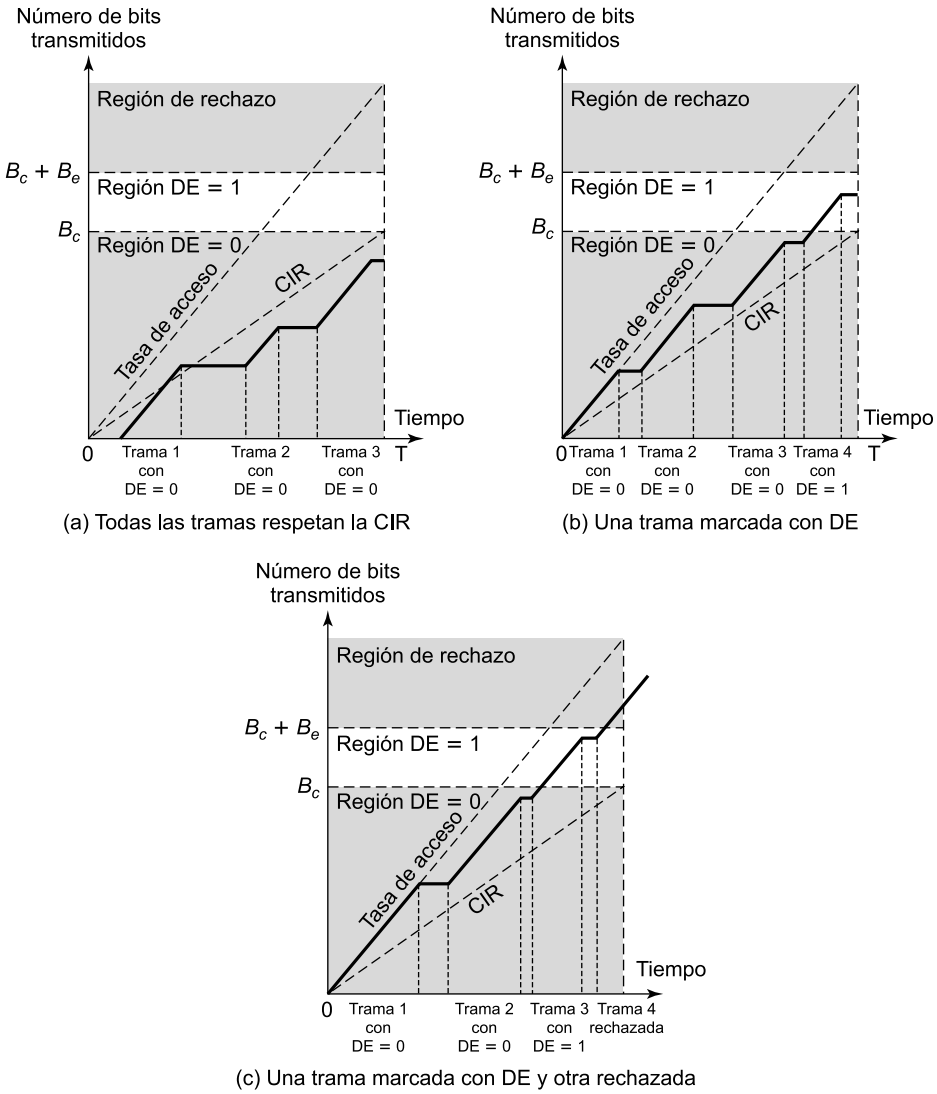


Figura 13.7. Ilustración de las relaciones entre los parámetros de congestión.

En la Figura 13.7, basada en una figura de la recomendación I.370 de ITU-T, se ilustra la relación entre estos parámetros. La línea continua en cada gráfica representa el número acumulado de bits de información transferidos a través de una conexión desde el instante de tiempo $T = 0$. La línea discontinua rotulada «tasa de acceso» representa la velocidad de datos del canal correspondiente a esta conexión. La línea discontinua rotulada «CIR» es la tasa de información contratada en el intervalo de medida T. Obsérvese que, cuando se va a transmitir una trama, la línea continua es paralela a la línea de tasa de acceso; cuando se transmite una trama a través de un canal, éste se dedica a la transmisión de dicha trama. Cuando no hay tramas que transmitir, la línea continua es horizontal.

En la parte (a) de la Figura 13.7 se muestra un ejemplo en el que se transmiten tres tramas durante el intervalo de medida y el número total de bits en las tres tramas es menor que B_c.

Fijémonos en el hecho de que, durante la transmisión de la primera trama, la velocidad de transmisión real supera temporalmente la CIR. Esto no tiene consecuencias, ya que el gestor de tramas está relacionado sólo con el número acumulado de bits transmitidos durante el intervalo completo. En la parte (b) de la figura, la última trama transmitida durante el intervalo provoca que el número acumulado de bits transmitidos supere B_c, por lo que el gestor de tramas activa el bit DE de la trama. En la parte (c) de la figura, la tercera trama excede B_c y se marca para su potencial rechazo, mientras que la cuarta trama excede $B_c + B_e$ y es descartada.

PREVENCIÓN DE LA CONGESTIÓN MEDIANTE SEÑALIZACIÓN EXPLÍCITA

Es deseable hacer tanto uso como sea posible de la capacidad disponible en una red de retransmisión de tramas conservando la capacidad de reaccionar de manera adecuada y controlada ante la congestión. Éste es el objetivo de las técnicas de prevención explícita de congestión. En términos generales, para llevar a cabo esta prevención, la red alerta a los sistemas finales acerca del aumento de la congestión en la red, de modo que éstos toman las medidas oportunas para reducir la carga introducida en la red.

Mientras se desarrollaban los estándares de prevención explícita de congestión, se consideraban dos estrategias generales [BERG91]. Algunos creían que la congestión se producía siempre de forma lenta y casi siempre en los nodos de salida. Otros observaron casos en los que la congestión aumentaba muy rápidamente en los nodos intermedios, precisándose acciones decisivas rápidas para prevenir la congestión de la red. Veremos que estas aproximaciones se reflejan, respectivamente, en las técnicas de prevención explícita de congestión hacia adelante y hacia atrás.

En la señalización explícita se usan dos bits en el campo de dirección de cada trama, pudiendo ser activado cada uno de ellos por cualquier gestor de tramas que detecte la congestión. Si un gestor de tramas recibe una trama en la que uno de estos bits o los dos están activados, no debe desactivar los bits antes de retransmitir la trama. Así pues, los bits constituyen señales desde la red hacia el usuario final. Estos dos bits son:

- **Notificación explícita de congestión hacia atrás (BECN, *Backward Explicit Congestion Notification*):** notifica al usuario acerca de la conveniencia de poner en marcha los procedimientos para evitar la congestión allí donde son aplicables para el tráfico en dirección opuesta a la de la trama recibida. Indica que las tramas que transmita el usuario a través de esta conexión lógica pueden encontrar recursos congestionados.
- **Notificación explícita de congestión hacia adelante (FECN, *Forward Explicit Congestion Notification*):** notifica al usuario acerca de la conveniencia de poner en marcha los procedimientos para evitar la congestión allí donde son aplicables para el tráfico en la misma dirección que la de la trama recibida. Indica que la trama, sobre su conexión lógica, ha encontrado recursos congestionados.

Veamos cómo se usan estos bits por parte de la red y del usuario. En primer lugar, para la **respuesta de la red**, es necesario que cada gestor de tramas supervise el comportamiento de sus colas. Si el tamaño de éstas comienza a crecer de forma peligrosa, se deberían activar los bits FECN o BECN, o una combinación de ellos, para tratar de reducir el flujo de tramas a través del gestor de tramas. La elección de los bits FECN o BECN puede estar determinada por el hecho de que los usuarios finales de una conexión lógica dada estén preparados para responder a uno o al otro, lo cual se puede definir en el momento de la configuración. En cualquier caso, el gestor de tramas puede decidir qué conexiones lógicas deben ser alertadas acerca de la congestión. Si la congestión se hace más seria se podría notificar a todas las conexiones lógicas a través de un gestor de tramas.

En las etapas más tempranas de la congestión, el gestor de tramas podría notificarlo sólo a aquellos usuarios cuyas conexiones generan la mayor parte del tráfico.

La **respuesta de usuario** se determina en base a la recepción de las señales BECN o FECN. El procedimiento más sencillo consiste en responder a la señal BECN: el usuario simplemente reduce la velocidad a la que transmite las tramas hasta que la señal cesa. La respuesta a la señal FECN es más compleja, ya que es necesario que el usuario notifique a su usuario paritario sobre esa conexión para que reduzca su flujo de tramas. Las funciones centrales usadas en el protocolo de retransmisión de tramas no contemplan esta notificación, por lo que debe ser realizada en una capa superior, como la de transporte. El control de flujo se podría también complementar con el protocolo de control LAPF o con algún otro protocolo de control de enlace implementado encima de la subcapa de retransmisión de tramas. El protocolo de control LAPF es especialmente útil, dado que incluye una mejora a LAPD que permite al usuario ajustar el tamaño de la ventana.

13.6. GESTIÓN DE TRÁFICO EN ATM

Debido a su alta velocidad y al pequeño tamaño de celda usado, las redes ATM presentan dificultades no existentes en otros tipos de redes para el control efectivo de la congestión. La complejidad del problema se debe al reducido número de bits suplementarios disponibles para llevar a cabo el control sobre el flujo de celdas de usuario. Este campo es en la actualidad un tema de intensa investigación, encontrándose aún en desarrollo diversas técnicas para el control de tráfico y de congestión. ITU-T, en el documento I.371, ha definido un conjunto restringido inicial de capacidades de control de tráfico y de congestión encaminadas hacia la consecución de mecanismos sencillos y eficiencias de red realistas. El Foro ATM ha publicado una versión algo más avanzada de este conjunto de capacidades en su especificación de gestión de tráfico 4.0 [ATM96]. Esta sección se centra en las especificaciones dadas por el Foro ATM.

Comenzaremos con una revisión del problema de la congestión y el sistema adoptado por ITU-T y el Foro ATM. Tras esto se discutirán algunas de las técnicas específicas desarrolladas para la gestión de tráfico y el control de congestión.

REQUISITOS PARA EL CONTROL DE TRÁFICO Y DE CONGESTIÓN EN ATM

Tanto los tipos de modelo de tráfico impuestos en redes ATM como las características de transmisión de este tipo de redes difieren en gran medida de los de otras redes de conmutación. La mayor parte de las redes de conmutación de paquetes y de retransmisión de tramas no transportan tráfico de datos de tiempo real. Generalmente, el tráfico sobre circuitos virtuales individuales o sobre conexiones de retransmisión de tramas es de naturaleza a ráfagas, esperando el sistema receptor la llegada del tráfico sobre cada conexión de esta forma. En consecuencia:

- La red no necesita replicar exactamente el patrón de tiempo del tráfico de entrada sobre el nodo de salida.
- Por tanto, se puede usar multiplexación estadística para dar cabida a varias conexiones lógicas sobre la interfaz física entre el usuario y la red. La velocidad de transmisión media necesaria en cada conexión es menor que la tasa de ráfagas para la conexión en cuestión, y la interfaz usuario-red (UNI, *User-Network Interface*) sólo precisa estar diseñada para una capacidad ligeramente superior que la suma de las velocidades promedio para todas las conexiones.

Existen numerosas herramientas para el control de congestión en redes de conmutación de paquetes y de retransmisión de tramas, algunas de las cuales se presentan a lo largo de este capítulo. Estos tipos de esquemas de control de congestión son inadecuados para redes ATM, citándose varias razones para ello en [GERS91]:

- La mayor parte del tráfico no está sujeto a control de flujo alguno. Por ejemplo, las fuentes de tráfico de voz y de vídeo no pueden parar de generar celdas aun cuando la red se encuentre congestionada.
- La realimentación es lenta debido a lo drásticamente reducido del tiempo de transmisión de celda en comparación con los retardos de propagación a través de la red.
- Las redes ATM soportan generalmente una amplia variedad de aplicaciones, las cuales requieren capacidades comprendidas entre unos pocos kbps y varias centenas de Mbps. Los esquemas de control de congestión relativamente simples generalmente acaban castigando un extremo o el otro del espectro.
- Las aplicaciones sobre redes ATM pueden dar lugar a patrones de tráfico diversos (por ejemplo, fuentes de velocidad constante frente a fuentes de velocidad variable). De nuevo, resulta difícil para las técnicas de control de congestión convencionales gestionar adecuadamente este tráfico.
- Aplicaciones distintas sobre redes ATM necesitan servicios de red diferentes (por ejemplo, servicio sensible al retardo para voz y vídeo y servicio sensible a las pérdidas para datos).
- Las elevadas velocidades de conmutación y transmisión hacen que las redes ATM sean más volubles, en términos de control de congestión y de tráfico. Un esquema que dependa fuertemente de las condiciones cambiantes producirá fluctuaciones extremas y desastrosas en la política de encaminamiento y en el control de flujo.

Dos cuestiones clave del funcionamiento relacionadas con los puntos anteriores son los efectos de la latencia/velocidad y la variación del retardo de celdas, las cuales pasamos a describir a continuación.

EFECTOS DE LATENCIA/VELOCIDAD

Considérese la transferencia de celdas ATM sobre una red de velocidad de 150 Mbps. A dicha velocidad se tardará $(53 \times 8 \text{ bits})/(150 \times 10^6 \text{ bps}) \approx 2{,}8 \times 10^{-6}$ segundos en insertar una sola celda en la red. El tiempo que se tarda en transmitir la celda desde el origen hasta el usuario destino dependerá del número de conmutadores ATM intermedios, del tiempo de conmutación en cada conmutador y del tiempo de propagación a lo largo de todos los enlaces que componen el camino entre el origen y el destino. Por sencillez, ignoremos los retardos de conmutación ATM y supongamos que la propagación se realiza a una velocidad igual a dos tercios la de la luz. Así, si el origen y el destino se encuentran situados en las costas opuestas de los Estados Unidos, el retardo de propagación del viaje de ida y vuelta será de 48×10^{-3} segundos.

En estas condiciones, supóngase que un emisor A lleva a cabo la transferencia de un fichero largo hacia un destino B y que se hace uso de control implícito de congestión (es decir, no existen notificaciones explícitas de congestión, sino que el emisor deduce la ocurrencia de congestión a partir de la pérdida de datos). Si la red pierde una celda debido a la congestión, B puede devolver un mensaje de rechazo a A, el cual debe retransmitir la celda perdida y, posiblemente, todas las

celdas siguientes. Pero debido al tiempo que tarda la notificación en llegar a A, éste ha transmitido N celdas adicionales, donde

$$N = \frac{48 \times 10^{-3} \text{ segundos}}{2{,}8 \times 10^{-6} \text{ segundos/celda}} = 1{,}7 \times 10^4 \text{ celdas} = 7{,}2 \times 10^6 \text{ bits}$$

Es decir, antes de que A pueda reaccionar ante la indicación de congestión se ha transmitido por encima de 7 megabits de datos.

Este cálculo ayuda a explicar por qué las técnicas que son adecuadas para la mayoría de las redes tradicionales no funcionan cuando se aplican a redes WAN ATM.

VARIACIÓN DEL RETARDO DE CELDAS

Para una red ATM, las señales de voz y de vídeo se pueden digitalizar y transmitir como una secuencia de celdas, lo que requiere, especialmente para voz, que los retardos en la red sean pequeños. Éste es generalmente el caso de las redes ATM, que, como ya se ha discutido, están diseñadas para minimizar el coste de transmisión y el procesamiento interno a la red, de forma que sea posible una conmutación de celdas y un encaminamiento muy rápidos.

Existe otro importante requisito que a veces entra en conflicto con el anterior: la velocidad de envío de celdas al usuario destino debe ser constante. Ahora bien, es inevitable que exista alguna variabilidad en la velocidad de transmisión de celdas debido a efectos internos a la red y en la UNI origen. A continuación se resumen estos efectos, considerándose en primer lugar cómo podría hacer frente el usuario destino a las variaciones del retardo de celdas en tránsito hacia él desde el usuario origen.

En la Figura 13.8 se muestra un procedimiento general para conseguir una velocidad constante (CBR). Sea $D(i)$ el retardo extremo a extremo experimentado por la celda i-ésima. El sistema destino no conoce el retardo exacto, dado que no existe sello de tiempo asociado a cada celda y, aun en

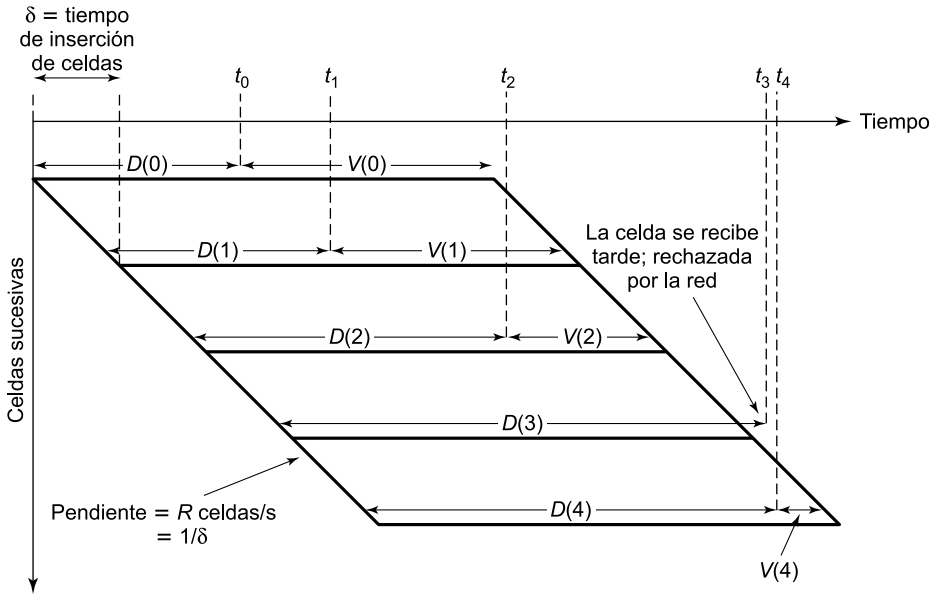


Figura 13.8. Tiempo de ensamblado de celdas CBR.

el caso de que lo hubiese, es imposible mantener perfectamente sincronizados los relojes del emisor y del receptor. Cuando se recibe en un instante de tiempo t_0 la primera celda de una conexión, el usuario retarda la celda una cantidad adicional $V(0)$ antes de enviarla a la aplicación. Esta cantidad, $V(0)$, es una estimación de la variación del retardo de celdas que puede tolerar la aplicación y que es probable que ocasione la red.

Las siguientes celdas se retrasan de manera que se transmiten hacia el usuario a una velocidad constante de R celdas por segundo, siendo, por tanto, $\delta = 1/R$ el tiempo entre envíos de celdas a la aplicación (tiempo transcurrido entre el comienzo del envío de una celda y el comienzo del envío de la siguiente). Para conseguir una velocidad constante, la siguiente celda es retrasada una cantidad variable $V(1)$ de modo que se satisfaga:

$$t_1 + V(1) = t_0 + V(0) + \delta$$

Así,

$$V(1) = V(0) - [t_1 - (t_0 + \delta)]$$

En general,

$$V(i) = V(0) - [t_i - (t_0 + i \times \delta)]$$

que se puede expresar también como

$$V(i) = V(i - 1) - [t_i - (t_{i-1} + \delta)]$$

Si el valor de $V(i)$ obtenido es negativo, se rechaza la celda. El resultado es que los datos se envían a la capa superior a una velocidad constante, con espaciados ocasionales debido a la pérdida de celdas.

El retardo inicial $V(0)$, que es también el retardo medio aplicado a todas las celdas entrantes, es función de la variación del retardo de celdas esperada. Para minimizar este retardo, un abonado debe solicitar del proveedor de la red una variación del retardo de celdas mínima, lo que nos lleva al siguiente compromiso: la variación del retardo de celdas se puede reducir aumentando la velocidad relativa a la carga en la UNI e incrementando los recursos en la red.

Contribución de la red a la variación del retardo de celdas

Una componente de la variación del retardo de celdas se debe a sucesos internos a la red. La variación del retardo de paquetes en redes de conmutación de paquetes puede ser considerable debido a los efectos de puesta en cola en cada uno de los nodos de conmutación intermedios y al tiempo de procesamiento necesario para analizar las cabeceras de los paquetes y llevar a cabo el encaminamiento. En menor medida, esto mismo ocurre con la variación del retardo de tramas en redes de retransmisión de tramas. Por su parte, en el caso de redes ATM es probable que las variaciones del retardo de celdas debidas a los efectos de la red sean inferiores incluso que en retransmisión de tramas. Las principales razones para ello son las siguientes:

- El protocolo ATM está diseñado para minimizar el procesamiento suplementario en los nodos de conmutación intermedios. Las celdas son de tamaño fijo con formatos de cabecera también fijos, no siendo necesarios procedimientos de control de errores ni de flujo.
- Para dar cabida a las altas velocidades de las redes ATM, los conmutadores ATM se han diseñado para ofrecer un rendimiento extremadamente alto. Así, el tiempo de procesamiento en un nodo para una celda individual es despreciable.

La congestión es el único factor que podría provocar variaciones importantes en el retardo de celdas. Si la red comienza a congestionarse, las celdas se pueden descartar o bien pueden ser puestas en cola en los conmutadores afectados. En consecuencia, es importante que la carga aceptada por la red en cualquier instante de tiempo sea tal que no cause congestión.

Variación del retardo de celdas en la UNI

Incluso si la aplicación transmite datos a una velocidad constante, la variación en el retardo de celdas puede producirse en el origen debido al procesamiento que tiene lugar en las tres capas del modelo ATM.

En la Figura 13.9 se ilustran las posibles causas de la variación del retardo de celdas. En este ejemplo, las conexiones ATM A y B soportan velocidades de transmisión de datos de usuario de X e Y Mbps, respectivamente ($X > Y$). Los datos se segmentan en el nivel AAL en bloques de 48 octetos. Obsérvese que, en un diagrama de tiempo, los bloques parecen de tamaño diferente para las dos conexiones; concretamente, el tiempo, en microsegundos, necesario para generar un bloque de 48 octetos de datos es:

$$\text{Conexión A: } \frac{48 \times 8}{X}$$

$$\text{Conexión B: } \frac{48 \times 8}{Y}$$

La capa ATM encapsula cada segmento en una celda de 53 octetos. Estas celdas se deben mezclar y enviar a la capa física para transmitirlas a la velocidad de transmisión del enlace. El retardo

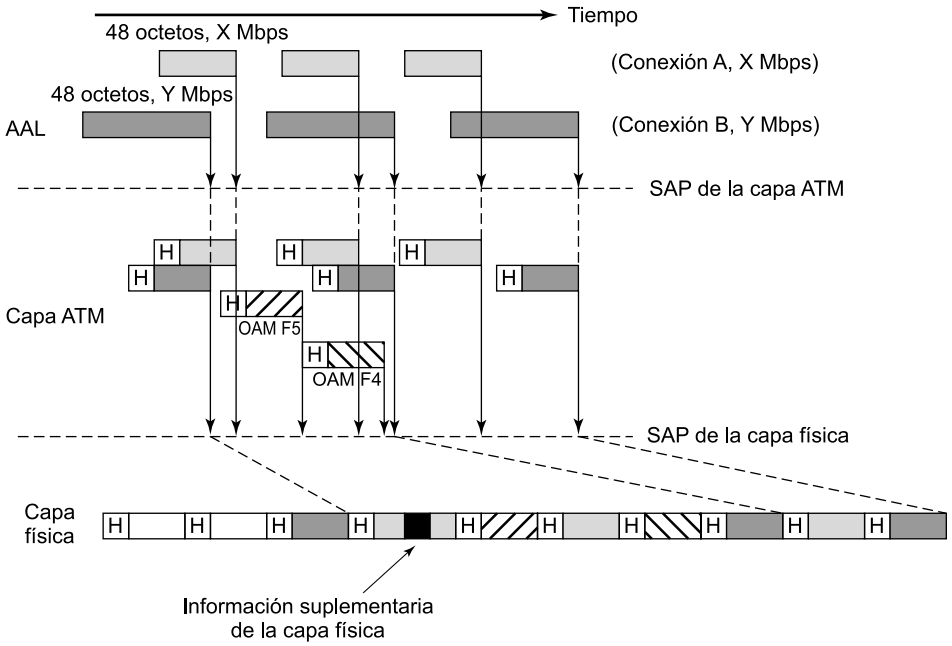


Figura 13.9. Orígenes de la variación del retardo de celdas (I.371).

se debe al proceso de entremezclado: si dos celdas de diferentes conexiones llegan a la capa ATM en tiempos solapados, una de las celdas debe ser retrasada en una cantidad igual al solapamiento. Además, la capa ATM genera celdas OAM (operación y mantenimiento) que deben ser mezcladas con celdas de usuario.

Es posible introducir retardos de celda adicionales en la capa física. Por ejemplo, si las celdas se transmiten en tramas SDH (jerarquía digital síncrona), los bits suplementarios de estas tramas se insertarán en el enlace físico, provocando un retardo en los bits de la capa ATM.

Ninguno de los retardos enunciados se puede predecir de forma exacta, y ninguno de ellos sigue un patrón repetitivo. En consecuencia, existe una componente aleatoria en el intervalo de tiempo entre la recepción de datos en la capa ATM desde la capa AAL y la transmisión de esos datos en una celda a través de la UNI.

CONTROL DE TRÁFICO Y DE CONGESTIÓN

El documento I.371 especifica los siguientes objetivos en el control de tráfico y de congestión en ATM:

- El control de tráfico y de congestión en la capa ATM debería permitir un número suficiente de clases de calidad de servicio (QoS) de la capa ATM para todos los servicios de red posibles; la especificación de estas clases de QoS debe ser consistente con las prestaciones de la red en estudio.
- El control de tráfico y de congestión en la capa ATM no debería depender de protocolos AAL específicos del servicio de red ni de protocolos de capas superiores que sean específicos de la aplicación. Los protocolos de capas superiores a la capa ATM pueden hacer uso de información proporcionada por esta capa para mejorar la utilidad que dichos protocolos pueden obtener de la red.
- El diseño de un conjunto óptimo de controles de tráfico y de congestión en la capa ATM debería minimizar la complejidad de la red y de los sistemas finales al tiempo que se maximiza la utilización de la red.

Para conseguir estos objetivos, ITU-T y el Foro ATM han definido una serie de funciones de control de tráfico y de congestión que operan en un rango dado de intervalos de tiempo. En la Tabla 13.2 se enumeran estas funciones con respecto a los tiempos de respuesta en los que operan. Se consideran cuatro niveles de tiempo:

- **Tiempo de inserción de celdas:** las funciones de este nivel reaccionan inmediatamente ante celdas transmitidas.
- **Tiempo de propagación de ida y vuelta:** en este nivel la red responde dentro del tiempo de vida de una celda en la red y puede realizar indicaciones al origen en forma de realimentación.
- **Duración de la conexión:** la red determina en este nivel si se puede establecer una nueva conexión con una QoS dada y qué nivel de prestaciones se fijará.
- **Término de larga duración:** son controles que afectan a más de una conexión ATM y se establecen para uso de larga duración.

La esencia de la estrategia de control de tráfico se basa (1) en la determinación de si se puede dar cabida a una nueva conexión ATM y (2) en el acuerdo con el abonado acerca de los parámetros de

prestaciones tolerados. En efecto, el abonado y la red llevan a cabo un contrato o acuerdo de tráfico: la red acepta transportar un tráfico con un nivel de prestaciones dado sobre esa conexión y el abonado acepta no exceder los límites de los parámetros de tráfico fijados. Las funciones de control de tráfico están relacionadas con el establecimiento y cumplimiento de estos parámetros de tráfico, por lo que están relacionadas con la prevención de la congestión. Si el control de tráfico falla en algunas situaciones, se puede producir congestión, en cuyo caso se invocan las funciones de control de congestión para responder y solventar el problema.

Tabla 13.2. Funciones de control de tráfico y de congestión.

Tiempo de respuesta	Funciones de control de tráfico	Funciones de control de congestión
Término de larga duración	• Gestión de recursos usando caminos virtuales	
Duración de conexión	• Control de admisión de conexiones (CAC)	
Tiempo de propagación de ida y vuelta	• Gestión rápida de recursos	• Indicación explícita de congestión hacia adelante (EFCI) • Control de flujo ABR
Tiempo de inserción de celdas	• Control de los parámetros de uso (UPC) • Control de prioridad • Adaptación de tráfico	• Rechazo selectivo de celdas

TÉCNICAS DE GESTIÓN DE TRÁFICO Y DE CONTROL DE CONGESTIÓN

ITU-T y el Foro ATM han definido un conjunto de funciones de gestión de tráfico para mantener la calidad del servicio (QoS) de las conexiones ATM. Las funciones de gestión de tráfico ATM hacen referencia al conjunto de acciones tomadas por la red para evitar las condiciones de congestión o minimizar los efectos de ésta. En esta sección se presentan las siguientes técnicas:

- Gestión de recursos haciendo uso de caminos virtuales.
- Control de admisión de conexiones.
- Control de los parámetros de uso.
- Rechazo selectivo de celdas.
- Adaptación del tráfico.

Gestión de recursos haciendo uso de caminos virtuales

El concepto fundamental en la gestión de recursos de red es la reserva de dichos recursos de manera que se separen los flujos de tráfico de acuerdo con las características del servicio. Hasta ahora, la única función de control de tráfico específica basada en la gestión de recursos de red definida por el Foro ATM hace uso de caminos virtuales.

Como se vio en el Capítulo 11, una conexión de camino virtual (VPC, *Virtual Path Connection*) proporciona una forma adecuada para llevar a cabo la agrupación de conexiones de canales virtuales (VCC, *Virtual Channel Connection*) similares. La red ofrece características conjuntas de

prestaciones y capacidad en el camino virtual, siendo compartidas por las conexiones virtuales. Se deben considerar tres casos:

- **Aplicación usuario-usuario:** la VPC se extiende entre un par de UNI. En este caso, la red no conoce la QoS de las VCC individuales en la VPC, de modo que es responsabilidad del usuario asegurar que la VPC pueda dar cabida a la demanda conjunta de las VCC.
- **Aplicación del usuario a la red:** la VPC se extiende entre una UNI y un nodo de la red. En este caso, la red conoce la QoS de las VCC en una VPC y debe darles cabida.
- **Aplicación red-red:** la VPC se extiende entre dos nodos de red. De nuevo, la red conoce la QoS de las VCC en la VPC y debe darles cabida.

Los parámetros de QoS más importantes relacionados con la gestión de los recursos de red son la tasa de pérdida de celdas, el retardo de transferencia de celdas y la variación del retardo de celdas, estando todos ellos afectados por la cantidad de recursos dedicados por la red a la VPC. Si una VCC se extiende a través de varias VPC, las prestaciones de la VCC dependen de las prestaciones de las VPC consecutivas y de cómo se gestiona la conexión en cualquier nodo que realice funciones relacionadas con las VCC. Este nodo puede ser un conmutador, un concentrador u otro equipo de red. Las prestaciones de cada VPC dependen de la capacidad de la VPC y de las características de tráfico de las VCC contenidas en la VPC. Las prestaciones de cada una de las funciones relacionadas con las VCC dependen de la velocidad de conmutación/procesamiento en el nodo y de la prioridad relativa con que se gestionan las distintas celdas.

En la Figura 13.10 se muestra un ejemplo. Las VCC 1 y 2 presentan unas prestaciones que dependen de las VPC b y c y de cómo se gestionan estas VCC en los nodos intermedios. Esto puede diferir de las prestaciones observadas en las VCC 3, 4 y 5.

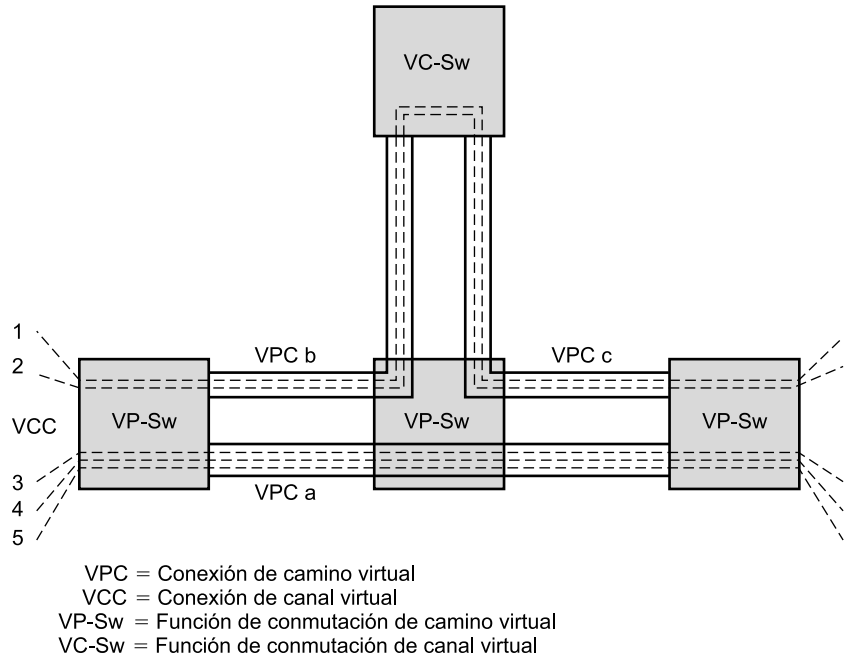


Figura 13.10. Configuración de VCC y VPC.

Existen varias alternativas en la manera de agrupar VCC y en el tipo de prestaciones que presentan. Si todas las VCC en una VPC se gestionan de forma similar, deberían experimentar prestaciones de red similares en términos de tasa de pérdida de celdas, de retardo de transferencia de celdas y de variación del retardo de celdas. Alternativamente, cuando VCC diferentes en la misma VPC requieren una QoS diferente, las prestaciones de la VPC acordadas entre la red y el abonado deberían ser alcanzables para la mayor parte de los requisitos VCC demandados.

En cualquier caso, cuando existen varias VCC en la misma VPC, la red tiene dos opciones para reservar capacidad para la VPC:

- **Demanda conjunta de pico:** la red puede establecer la capacidad (velocidad) de la VPC a un valor igual a la suma de las velocidades de pico de todas las VCC en la VPC. La ventaja de esta aproximación es que cada VCC puede presentar una QoS que dé cabida a su demanda de pico. Por el contrario, la desventaja radica en que la capacidad de la VPC no se utiliza completamente durante la mayor parte del tiempo y, en consecuencia, algunos recursos de la red estarán infrautilizados.

- **Multiplexación estadística:** si la red especifica la capacidad de la VPC a un valor mayor o igual que la suma de las velocidades promedio de las VCC pero menor que la demanda de pico conjunta, se ofrece un servicio de multiplexación estadística. Con esta técnica de multiplexación, las VCC experimentan una variación del retardo de celdas y un retardo de transferencia de celdas superiores. Dependiendo del tamaño de las memorias temporales usadas en las colas de transmisión de celdas, las VCC pueden experimentar también una mayor tasa de pérdida de celdas. Esta aproximación tiene la ventaja de utilizar la capacidad de forma más eficiente, resultando atractiva si las VCC pueden tolerar la QoS inferior.

Cuando se usa multiplexación estadística es preferible agrupar las VCC en varias VPC bajo la consideración de características de tráfico y necesidad de QoS similares. Si VCC diferentes comparten la misma VPC y se usa multiplexación estadística, es difícil ofrecer un acceso adecuado simultáneamente a las secuencias de bajo y de alto tráfico.

Control de admisión de conexiones

El control de admisión de conexiones es la primera línea de defensa de autoprotección de la red ante una carga excesiva. En esencia, cuando un usuario solicita una VCC o una VPC nuevas, debe especificar (implícita o explícitamente) las características de tráfico para la conexión en ambos sentidos. El usuario selecciona las características de tráfico mediante la elección de una QoS de entre las clases que ofrece la red. La red acepta la conexión sólo si puede conseguir los recursos necesarios para admitir el nivel de tráfico, al tiempo que mantiene la QoS convenida en las conexiones existentes. Al aceptar la conexión, la red establece un *contrato de tráfico* con el usuario. Una vez aceptada la conexión, la red continúa ofreciendo la QoS convenida mientras el usuario respete el acuerdo de tráfico.

El acuerdo o contrato de tráfico puede consistir en los cuatro parámetros definidos en la Tabla 13.3: velocidad de pico de celdas (PCR, *Peak Cell Rate*), variación del retardo de celdas (CDV, *Cell Delay Variation*), velocidad sostenible de celdas (SCR, *Sustainable Cell Rate*) y tolerancia a ráfagas. Con fuentes de velocidad constante (CBR, *Constant Bit Rate*), sólo son relevantes los dos primeros parámetros, pudiéndose utilizar los cuatro cuando se trabaja con fuentes de velocidad variable (VBR, *Variable Bit Rate*).

Tabla 13.3. Parámetros de tráfico usados en la definición de la QoS de VCC/VPC.

Parámetro	Descripción	Tipo de tráfico
Velocidad de pico de celdas (PCR)	Límite superior de tráfico que puede presentarse en una conexión ATM	CBR, VBR
Variación del retardo de celdas (CDV)	Límite superior de la variabilidad en el patrón de recepción de celdas observado en un único punto de medida en referencia a la velocidad de pico de celdas	CBR, VBR
Velocidad sostenible de celdas (SCR)	Límite superior de la velocidad media de una conexión ATM, calculado sobre la duración de la conexión	VBR
Tolerancia a ráfagas	Límite superior de la variabilidad en el patrón de recepción de celdas observado en un único punto de medida en referencia a la velocidad sostenible de celdas	VBR

CBR = velocidad constante
VBR = velocidad variable

Como sugiere el nombre, la velocidad de pico de celdas es la máxima velocidad a la que se generan en el origen las celdas para una conexión dada. Sin embargo, hemos de tener en consideración la variación del retardo de celdas. Aunque un emisor puede generar celdas a una velocidad de pico constante, las variaciones del retardo de celdas debidas a diversos factores (*véase* Figura 13.9) afectarán a la evolución temporal, provocando la agrupación y separación de celdas. Así pues, una fuente puede exceder temporalmente la velocidad de pico de celdas debido a la agrupación. Para que la red reserve adecuadamente recursos para esta conexión debe conocer no sólo la velocidad de pico de celdas, sino también la CDV.

La relación exacta entre la velocidad de pico de celdas y la CDV depende de las definiciones operacionales de estos dos términos. El estándar establece estas definiciones en términos de un algoritmo de velocidad de celdas. Dado que el algoritmo se puede usar para el control de los parámetros de uso, pospondremos su estudio hasta el siguiente apartado.

Los parámetros PCR y CDV deben especificarse para cada conexión. Como opción para fuentes de velocidad variable, el usuario puede especificar también una velocidad sostenible de celdas y una tolerancia a la aparición de ráfagas. Estos parámetros son análogos a PCR y CDV, respectivamente, pero aplicados a una velocidad de generación de celdas promedio en lugar de a una velocidad de pico. El usuario puede describir el flujo futuro de celdas en mayor detalle mediante el uso de los parámetros SCR y tolerancia a ráfagas así como mediante PCR y CDV. Con esta información adicional, la red podría utilizar más eficientemente sus recursos; por ejemplo, si se multiplexan estadísticamente varias VCC sobre una VPC, el conocimiento de las velocidades promedio y de pico de celdas posibilita a la red la reserva de memoria temporal de capacidad suficiente para la gestión eficaz del tráfico sin pérdida de celdas.

Para una conexión dada (VPC o VCC), los cuatro parámetros de tráfico se pueden especificar de formas distintas según se ilustra en la Tabla 13.4. Los valores de los parámetros se pueden definir implícitamente mediante reglas impuestas por el operador de la red. En este caso, se les asignan los mismos valores a todas las conexiones, o a todas las conexiones de una misma clase se les

asigna el valor de esta clase. El operador de red puede asociar también valores de parámetros a un abonado dado y asignarlos en el momento de la suscripción; asimismo, los valores de los parámetros para una conexión particular se pueden asignar en el momento de la conexión. En el caso de una conexión virtual permanente, estos valores son asignados por la red cuando se establece la conexión. Para una conexión virtual conmutada, los parámetros son negociados entre el usuario y la red mediante un protocolo de señalización.

Tabla 13.4. Procedimientos usados para establecer los valores de los parámetros de tráfico contratados

	Parámetros especificados explícitamente		**Parámetros especificados implícitamente**
	Valores de parámetros especificados en el momento del establecimiento de la conexión	**Valores de parámetros especificados en el momento de la suscripción**	**Valores de parámetros especificados usando reglas por defecto**
	Requerido por el usuario/NMS	**Asignados por el operador de la red**	
SVC	Señalización	Mediante suscripción	Reglas por defecto red-operador
PVC	NMS	Mediante suscripción	Reglas por defecto red-operador

SVC = conexión virtual conmutada
PVC = conexión virtual permanente
NMS = sistema de gestión de red

Otro aspecto de la calidad del servicio que se puede solicitar o asignar para una conexión dada es la prioridad de pérdida de celdas. Un usuario puede solicitar dos niveles de prioridad de pérdida de celdas para una conexión ATM, indicándose la prioridad de una celda individual mediante el bit CLP existente en su cabecera (*véase* Figura 11.4). Cuando se usan dos niveles de prioridad, se deben especificar los parámetros de tráfico para ambos flujos de celdas. Esto se realiza, generalmente, mediante la especificación de un conjunto de parámetros de tráfico para tráfico de alta prioridad (CLP = 0) y un conjunto de parámetros de tráfico para todo tipo de tráfico (CLP = 0 o 1). Basándose en este análisis, la red puede llevar a cabo la reserva de recursos de forma más eficiente.

Control de los parámetros de uso

Una vez que la conexión ha sido aceptada por la función de control de admisión de conexiones, la función de control de parámetros de uso (UPC, *Usage Parameter Control*) de la red supervisa la conexión para determinar si el tráfico está en concordancia con el contrato de tráfico acordado. El objetivo principal del control de los parámetros de uso es proteger los recursos de la red ante la producción de una sobrecarga en una conexión, lo que afectaría adversamente la QoS en otras conexiones, a través de la detección de violaciones en los parámetros asignados y tomando las medidas oportunas.

El control de los parámetros de uso se puede realizar tanto a nivel de camino virtual como a nivel de canal virtual. El más importante de ellos es el control a nivel VPC, ya que los recursos de la red se reservan inicialmente, en general, en base a caminos virtuales, con la capacidad del camino virtual compartida entre los diferentes canales virtuales miembros.

Existen dos funciones distintas asociadas al control de los parámetros de uso:

- Control de la velocidad de pico de celdas y de la variación del retardo de celdas asociada (CDV).
- Control de la velocidad sostenible de celdas y de la tolerancia a la aparición de ráfagas.

Consideremos en primer lugar la velocidad de pico de celdas y la variación del retardo de celdas asociada. En términos sencillos, se dice que un tráfico es adecuado si la velocidad de pico de transmisión de celdas no excede la velocidad de pico de celdas acordada, sujeta a la posibilidad de que la variación del retardo de celdas se encuentre en el rango establecido. El documento I.371 define un algoritmo, el algoritmo de velocidad de pico de celdas, que supervisa el acuerdo en base a dos parámetros: la velocidad de pico de celdas, R, y el límite de tolerancia CDV, τ. Así, $T = 1/R$ es el intervalo de tiempo entre llegada de celdas si no hay CDV. En caso de que exista CDV, T es el tiempo promedio entre llegada de celdas a la velocidad de pico. El algoritmo se ha definido para supervisar la velocidad a la que llegan las celdas y para asegurar que el tiempo entre llegada de celdas no sea demasiado pequeño para provocar que el flujo exceda la velocidad de pico de celdas en una cantidad superior al límite de tolerancia.

El mismo algoritmo, con parámetros distintos, se puede usar para supervisar la velocidad sostenible de celdas R_s y la tolerancia de aparición de ráfagas asociada τ_s.

El algoritmo de velocidad de celdas es bastante complejo, pudiéndose encontrar los detalles en [STAL99b]. Este algoritmo define simplemente una forma de supervisar el cumplimiento del contrato de tráfico. Para llevar a cabo el control de los parámetros de uso, la red debe actuar de acuerdo con los resultados del algoritmo, consistiendo la estrategia más sencilla en aceptar las celdas que cumplen con los parámetros, descartándose por la función UPC aquellas que no los cumplen.

Las celdas que no cumplen con el contrato de tráfico pueden ser marcadas a opción de la red. En este caso, una celda que no cumple con el contrato se puede marcar con CLP = 1 (baja prioridad) y aceptarse, pudiendo ser descartada de la red posteriormente en caso de congestión.

La situación resulta más compleja en caso de que el usuario haya negociado dos niveles de prioridad de pérdida de celdas para una red. Recordemos que el usuario puede negociar un contrato para tráfico de alta prioridad (CLP = 0) y un contrato distinto para tráfico conjunto (CLP 0 o 1). Se aplican las siguientes reglas:

1. Una celda con CLP = 0 que cumple el contrato de tráfico para CLP = 0 es aceptada.
2. Una celda con CLP = 0 que no cumple el contrato para tráfico (CLP = 0) pero sí para tráfico (CLP 0 o 1) es marcada y aceptada.
3. Una celda con CLP = 0 que no cumple el contrato para tráfico (CLP = 0) ni para tráfico (CLP 0 o 1) es rechazada.
4. Una celda con CLP = 1 que cumple el contrato para tráfico (CLP = 0 o 1) es aceptada.
5. Una celda con CLP = 1 que no cumple el contrato para tráfico (CLP = 0 o 1) es rechazada.

Rechazo selectivo de celdas

El rechazo selectivo de celdas se lleva a cabo cuando la red, de forma independiente a la función UPC, rechaza celdas (CLP = 1). El objetivo es el rechazo de celdas de prioridad baja durante la congestión para salvaguardar las prestaciones de las celdas de prioridad superior. Obsérvese que la red no tiene forma de discriminar entre celdas marcadas como de baja prioridad por el emisor y celdas marcadas por la función UPC.

Adaptación del tráfico

El algoritmo UPC es una forma de **política de tráfico**, la cual se produce cuando se regula un flujo de datos de manera que las celdas (o las tramas o los paquetes) que superen un cierto nivel de prestaciones sean rechazadas o marcadas. Puede ser deseable complementar una política de tráfico con una de **adaptación del tráfico**, usada para suavizar el flujo de tráfico y reducir la agrupación de celdas. Esto puede dar lugar a una reserva de recursos más adecuada y a un tiempo de retardo medio reducido.

Una aproximación sencilla para llevar a cabo la adaptación del tráfico consiste en usar una variante del algoritmo UPC conocida como cubo de permisos. En contraste con el algoritmo UPC, que se limita a supervisar el tráfico y marcar o rechazar las celdas que no cumplen el contrato, la adaptación del tráfico mediante cubo de permisos controla el flujo de celdas que sí cumplen el contrato de tráfico.

En la Figura 13.11 se ilustra el principio básico del método de cubo de permisos. Un generador de permisos produce éstos a una velocidad de ρ permisos por segundo y los coloca en el cubo de permisos, el cual tiene una capacidad máxima de β permisos. Las celdas recibidas desde el emisor se sitúan en una memoria temporal con una capacidad máxima de K celdas. Para llevar a cabo la transmisión de una celda a través de un servidor es necesario coger un permiso del cubo, de modo que si el cubo se encuentra vacío, la celda se pone en cola en espera del siguiente permiso. El resultado de este esquema es que si existe un exceso de celdas y el cubo está vacío, las celdas se emiten con un flujo homogéneo de ρ celdas por segundo sin variación en el retardo de celdas hasta que se elimine el exceso. Por tanto, el cubo de permisos suaviza las ráfagas de celdas.

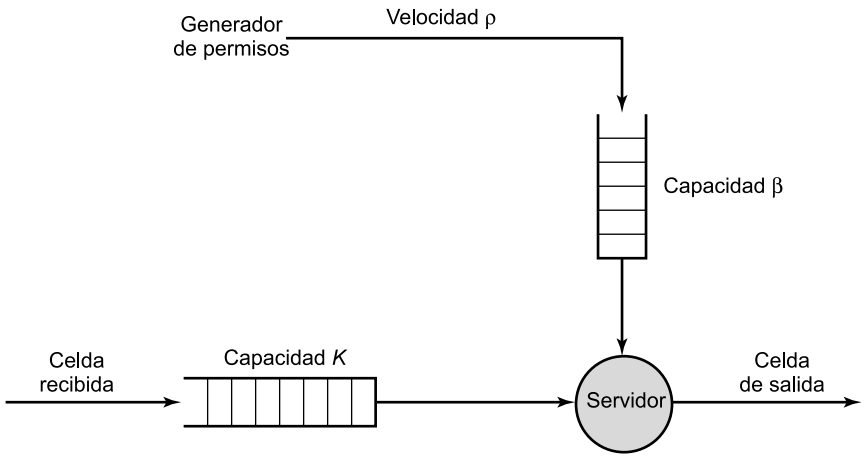


Figura 13.11. Cubo de permisos para adaptación de tráfico.

13.7. GESTIÓN DE TRÁFICO GFR EN ATM

La tasa de tramas garantizada (GFR, *Guaranteed Frame Rate*) proporciona un servicio tan simple como UBR (*Unspecified Bit Rate*) desde el punto de vista de los sistemas finales, a la vez que los requisitos introducidos en los elementos de la red ATM en términos de complejidad de procesamiento y sobrecarga son relativamente modestos. Esencialmente, con GFR, un sistema final no establece políticas para el tráfico que transmite ni necesita adaptarlo, sino que sencillamente puede

transmitir a la velocidad del enlace del adaptador ATM. Al igual que sucede en el caso de UBR, no existe garantía alguna de que la trama sea entregada correctamente. Es responsabilidad de alguna capa superior, como TCP, la adaptación a situaciones de congestión que pueden ocasionar la pérdida de tramas mediante la gestión de la ventana de transmisión y las técnicas de control de congestión presentadas en la Parte V. Al contrario que UBR, GFR permite al usuario reservar una cierta cantidad de capacidad, en términos de tasa de celdas, para cada VC GFR. Esta reserva garantiza una velocidad de transmisión mínima sin pérdidas por parte de la aplicación del usuario. Si la red no se encuentra congestionada, el usuario podrá transmitir a una velocidad mayor.

Una característica distintiva de GFR es que requiere que la red sea capaz de manejar tanto celdas como tramas. En condiciones de congestión, la red optará por descartar tramas completas en lugar de celdas individuales. Más aún, GFR requiere que todas las celdas que componen una trama compartan el mismo valor para el bit CLP. De esta forma, las tramas AAL 5 con CLP = 1 reciben un tratamiento de baja prioridad, siendo transmitidas según el criterio de mejor esfuerzo. Alternativamente, la capacidad mínima garantizada se aplica a las tramas CLP = 0.

Los parámetros que definen el acuerdo de tráfico en GFR son los siguientes:

- Velocidad pico de celdas (PCR, *Peak Cell Rate*).
- Velocidad mínima de celdas (MCR, *Minimum Cell Rate*).
- Tamaño máximo de ráfaga (MBS, *Maximum Burst Size*).
- Tamaño máximo de trama (MFS, *Maximum Frame Size*).
- Tolerancia a la variación del retardo de celdas (CDVT, *Cell Delay Variation Tolerance*).

MECANISMOS DE SOPORTE DE TASAS GARANTIZADAS

Existen tres aproximaciones básicas que pueden ser utilizadas por la red para proporcionar garantías en GFR a cada VC, permitiendo así a un conjunto de usuarios utilizar eficientemente y compartir de manera adecuada la capacidad disponible de la red [GOYA98]:

- Etiquetado y aplicación de la política.
- Gestión de las memorias intermedias.
- Planificación.

Estos elementos se pueden combinar de diversas formas en los elementos de una red ATM para producir una serie de implementaciones GFR posibles. En la Figura 13.12 se ilustra su uso.

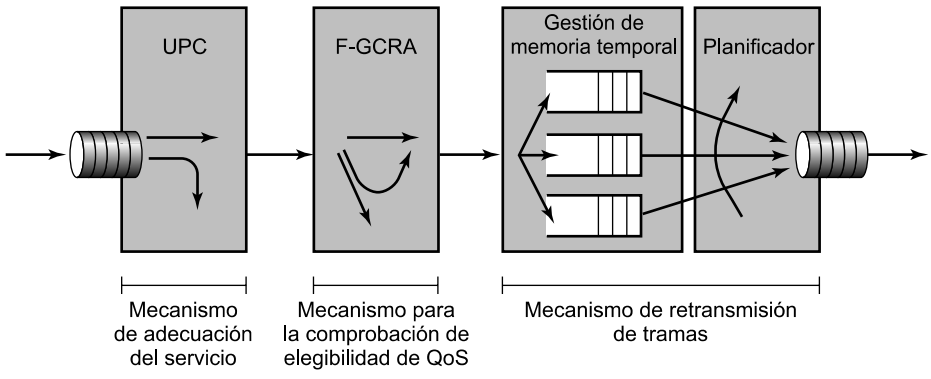


Figura 13.12. Componentes fundamentales de un mecanismo GFR [ANDR99].

Etiquetado y aplicación de la política

El etiquetado se emplea para discriminar entre aquellas tramas que se adecúan al acuerdo de tráfico GFR y aquellas que no. Los elementos de la red que llevan a cabo la comprobación establecen el bit CLP = 1 en todas las celdas de las tramas que violen el acuerdo. Dado que se acepta que las celdas etiquetadas no se ajustan al acuerdo de tráfico subscrito, éstas recibirán una calidad de servicio inferior a la de las celdas no etiquetadas por parte de los mecanismos de aplicación posterior, como la gestión de las memorias intermedias y la planificación. El etiquetado puede ser efectuado por la red, especialmente por el elemento en el punto de entrada a la red ATM, aunque también es posible que la fuente de datos lo lleve a cabo para señalar tramas de menor importancia.

La red, bien en el punto de acceso o bien en cualquier otro elemento de conmutación ATM, puede optar por descartar las celdas de las tramas que no se ajusten al acuerdo de tráfico (es decir, aquellas con CLP = 1), aunque las cuestiones relativas al descarte de celdas se consideran parte de la política de la red.

Gestión de las memorias intermedias

Los mecanismos de gestión de las memorias intermedias se encargan del tratamiento que reciben las celdas que han sido puestas en cola en un conmutador de la red o que han llegado a éste y deben ser almacenadas en la memoria temporal antes de su retransmisión. Cuando se alcanza una situación de congestión, manifestada por un alto nivel de ocupación de las memorias, los elementos de la red descartarán las celdas etiquetadas, otorgando así preferencia a las no etiquetadas. En concreto, un elemento de red podrá descartar celdas etiquetadas que estén ocupando espacio en las memorias temporales para dejar lugar disponible para las no etiquetadas. Con objeto de gestionar de forma apropiada y eficiente los recursos de memoria, un elemento de red puede llevar a cabo la asignación de memoria temporal de forma individual para cada VC, dedicando cierta cantidad de espacio a cada VC. Basándose en los acuerdos de tráfico establecidos para cada VC y en los niveles de ocupación de memoria temporal producidos por cada uno de ellos, el elemento de red puede tomar decisiones sobre el descarte de celdas; o dicho de otra forma, la decisión de descartar celdas se puede basar en umbrales de ocupación específicos para cada cola.

Planificación

Una función de planificación puede, como mínimo, dar un tratamiento preferencial a las celdas no etiquetadas sobre las etiquetadas. Asimismo, la red puede mantener colas separadas para cada VC y tomar decisiones de planificación diferentes para cada VC distinto. Se puede usar una disciplina de cola del tipo primero-en-llegar, primero-en-ser-servido dentro de cada cola, tal vez modificada para proporcionar mayor prioridad a las tramas del tipo CLP = 0. La planificación entre colas proporciona a la red un mecanismo de control sobre la tasa de salida de cada VC individual, permitiendo así una asignación de recursos adecuada para cada uno de ellos a la vez que se garantizan los requisitos de velocidad de tráfico mínima establecidos en el acuerdo con cada VC.

DEFINICIÓN DE ADECUACIÓN GFR

La primera función indicada en la Figura 13.12 es la función UPC. Ésta se encarga de monitorizar cada VC activo para asegurar que el tráfico de cada conexión se ajusta al acuerdo de tráfico, etiquetando o descartando las celdas que no se adecúen al mismo.

Una trama es adecuada si todas sus celdas lo son, y no es adecuada si una o más celdas no lo son. Se deben satisfacer tres condiciones para que una celda sea adecuada:

1. La tasa de celdas debe estar comprendida entre los límites suscritos en el acuerdo.
2. Todas las celdas de una trama deben tener el mismo valor CLP. Por tanto, el bit CLP de la celda monitorizada debe estar fijado al mismo valor que el de la primera celda de la trama.
3. La trama a la que pertenece la celda debe satisfacer el parámetro MFS. La validez de esta condición se puede asegurar comprobando en cada celda que, o bien es la última de la trama, o bien el número de celdas en la trama hasta ahora, e incluyendo ésta, es menor que MFS.

MECANISMO PARA LA COMPROBACIÓN DE ELEGIBILIDAD DE QoS

En los dos primeros bloques de la Figura 13.12 se muestra lo que se dispone como un proceso de filtrado en dos etapas. En primer lugar, las tramas son examinadas para comprobar su adecuación al acuerdo de tráfico. Las tramas que no se adecúan pueden ser descartadas inmediatamente. En caso de que no sea descartada, las celdas de una trama que no se ajusta al acuerdo de tráfico serán etiquetadas (CLP = 1), convirtiéndose así en susceptibles de ser eliminadas más adelante en la red. Por tanto, esta primera etapa es la encargada de garantizar que el tráfico se encuentre por debajo de un límite superior, penalizando aquellas celdas que hacen al flujo de tráfico rebasar este límite.

La segunda etapa de filtrado determina qué tramas cumplen los requisitos para las garantías de QoS bajo el acuerdo GFR para un VC dado. Para ello se supervisa un límite inferior de tráfico durante un cierto periodo de tiempo, seleccionando como tramas candidatas para la gestión de QoS a aquellas que conforman un flujo de tráfico por debajo del límite fijado.

Las tramas que se transmiten sobre un VC GFR pertenecen, por tanto, a una de las tres categorías siguientes:

- **Trama no adecuada:** las celdas de esta trama serán etiquetadas o descartadas.
- **Tramas adecuadas pero no elegibles:** compuestas por celdas que recibirán un servicio del tipo mejor esfuerzo.
- **Tramas adecuadas y elegibles:** compuestas por celdas que recibirán una garantía de entrega.

Para determinar la elegibilidad se utiliza una variante del algoritmo de tasa de celdas comentado en la Sección 13.6. Aunque la red puede descartar o etiquetar cualquier celda que no sea elegible, TM 4.1 establece que se espera de las implementaciones que intenten entregar el tráfico adecuado pero no elegible según la cantidad de recursos disponibles, con cada conexión GFR sobre un enlace compartiendo adecuadamente el ancho de banda local residual. No obstante, la especificación no intenta definir un criterio mediante el cual determinar si una implementación dada cumple la expectativa que acabamos de mencionar.

13.8. LECTURAS RECOMENDADAS

En [YANG95] se lleva a cabo una revisión exhaustiva de las técnicas de control de congestión. Por su parte, [JAIN90] y [JAIN92] proporcionan una discusión excelente acerca de los requisitos del control de congestión, de los distintos enfoques que se pueden tomar, así como distintas considera-

ciones sobre prestaciones. [KLEI93] proporciona una discusión excelente acerca de cuestiones de rendimiento en redes de datos. Aunque ligeramente anticuada, la referencia fundamental sobre control de flujo es [GERL80].

[GARR96] presenta una exposición razonada de las clases de servicios ATM y discute las implicaciones de cada una de ellas en la gestión de tráfico. En [MCDY99] se realiza una descripción detallada del control de tráfico en ATM para los servicios CBR y VBR. Por su parte, los textos [GIRO99] y [SCHW96] constituyen excelentes tratamientos de las características y prestaciones del tráfico ATM.

En [ANDR99] se ofrece una descripción clara y detallada de GFR. Otra descripción muy útil es [BONA01].

Finalmente, en [CHEN89] y [DOSH88] se presenta un interesante estudio de las cuestiones relativas al control de congestión en retransmisión de tramas. Referencias excelentes en esta materia son también [BUCK00], [GORA99] y [BLAC98].

ANDR99 Andrikopoulos, I.; Liakopoulous, A.; Pavlou, G.; y Sun, Z. «Providing Rate Guarantees for Internet Application Traffic Across ATM Networks.» *IEEE Communications Surveys*, Third Quarter 1999.http://www.comsoc.org/pubs/surveys.

BLAC98 Black, U. *Frame Relay Networks*. New York: McGraw-Hill, 1998.

BONA01 Bonaventure, O., y Nelissen, J. «Guaranteed Frame Rate: A Better Service for TCP/IP in ATM Networks.» *IEEE Network*, enero/febrero 2001.

BUCK00 Buckwalter, J. *Frame Relay: Technology and Practice.* Reading, MA: Addison-Wesley, 2000.

CHEN89 Chen, K.; Ho, K.; y Saksena, V. «Analysis and Design of a Highly Reliable Transport Architecture for ISDN Frame-Relay Networks.» *IEEE Journal on Selected Areas in Communications*, octubre 1989.

DOSH88 Doshi, B., y Nguyen, H. «Congestion Control in ISDN Frame-Relay Networks.» *AT&T Technical Journal,* noviembre/diciembre 1988.

GARR96 Garrett, M. «A Service Architecture for ATM: From Applications to Scheduling.» *IEEE Network*, mayo/junio 1996.

GERL80 Gerla, M., y Kleinrock, L. «Flow Control: A Comparative Survey.» *IEEE Transactions on Communications*, abril 1980.

GIRO99 Giroux, N., y Ganti, S. *Quality of Service in ATM Networks*. Upper Saddle River, NJ: Prentice Hall, 1999.

GORA99 Goralski, W. *Frame Relay for High-Speed Networks*. New York: Wiley, 1999.

JAIN90 Jain, R. «Congestion Control in Computer Networks: Issues and Trends.» *IEEE Network Magazine*, mayo 1990.

JAIN92 Jain, R. «Myths About Congestion Management in High-Speed Networks.» *Internetworking: Research and Experience,* volumen 3, 1992.

KLEI93 Kleinrock, L. «On the Modeling and Analysis of Computer Networks.» *Proceedings of the IEEE*, agosto 1993.

MCDY99 McDysan, D., y Spohn, D. *ATM: Theory and Application.* New York: McGraw-Hill, 1999.

SCHW96 Schwartz, M. *Broadband Integrated Networks*. Upper Saddle River, NJ: Prentice Hal PTR, 1996.

YANG95 Yang, C., y Reddy, A. «A Taxonomy for Congestion Control Algorithms in Packet Switching Networks.» *IEEE Network*, julio/agosto 1995.

13.9. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

calidad de servicio (QoS)
congestión
contrapresión
control de congestión
gestión de tráfico
paquete de obstrucción
reservas
señalización explícita de congestión
señalización implícita de congestión
variación del retardo de celdas

CUESTIONES DE REPASO

13.1. ¿Qué estrategias generales pueden ser usadas cuando un nodo sufre saturación en cuanto a los paquetes que recibe?

13.2. ¿Por qué tiende el retardo a infinito cuando la carga de la red excede la capacidad de la misma?

13.3. Proporcione una breve explicación de cada una de las técnicas de control de congestión ilustradas en la Figura 13.5.

13.4. ¿Cuál es la diferencia entre la señalización explícita de congestión hacia atrás y hacia delante?

13.5. Explique brevemente las tres aproximaciones generales para la señalización explícita de congestión.

13.6. Explique el concepto de tasa de información contratada (CIR) en redes de retransmisión de tramas.

13.7. ¿Qué implica la variación del retardo de celdas en una red ATM?

13.8. ¿Qué funciones se incluyen en el control de los parámetros de uso en ATM?

13.9. ¿Cuál es la diferencia entre la aplicación de políticas al tráfico y la adaptación de tráfico?

EJERCICIOS

13.1. Una técnica de control de congestión propuesta es la conocida como control isarrítmico. En este método se fija un número total de tramas en tránsito mediante la inserción en la red de un número fijo de permisos. Estos permisos circulan de forma aleatoria a través de la red de retransmisión de tramas. Cuando un gestor de tramas desea transmitir una trama procedente de un usuario conectado a él, debe primero capturar y destruir un permiso. Una vez que la trama se ha enviado hacia el usuario destino por el gestor de tramas al que éste se encuentra conectado, dicho gestor restituye el permiso. Indique tres problemas potenciales de esta técnica.

13.2. En el estudio de los efectos de latencia/velocidad presentado en la Sección 13.5 se vio un ejemplo en el que se transmitían alrededor de 7 megabits antes de que el emisor pudiese reaccionar. ¿Es que una técnica de control de flujo de ventana deslizante, como la descrita para HDLC, no se encuentra diseñada para solucionar los elevados retardos de propagación?

13.3. Considere la red de retransmisión de tramas mostrada en la Figura 13.13. C es la capacidad de un enlace en tramas por segundo. El nodo A presenta una carga constante de 0,8 tramas por segundo con destino a A'. Por su parte, el nodo B presenta una carga λ hacia B'. El nodo S dispone de un conjunto de memorias temporales comunes usadas tanto para el tráfico hacia A' como para el tráfico hacia B'. Cuando se llena la memoria temporal, las tramas se rechazan y se retransmiten posteriormente por el usuario origen. S tiene una capacidad de 2. Dibuje el rendimiento total (es decir, la suma de tráfico entre A y A' y entre B y B') en función de λ. ¿Qué fracción de rendimiento corresponde a tráfico A-A' para $\lambda > 1$?

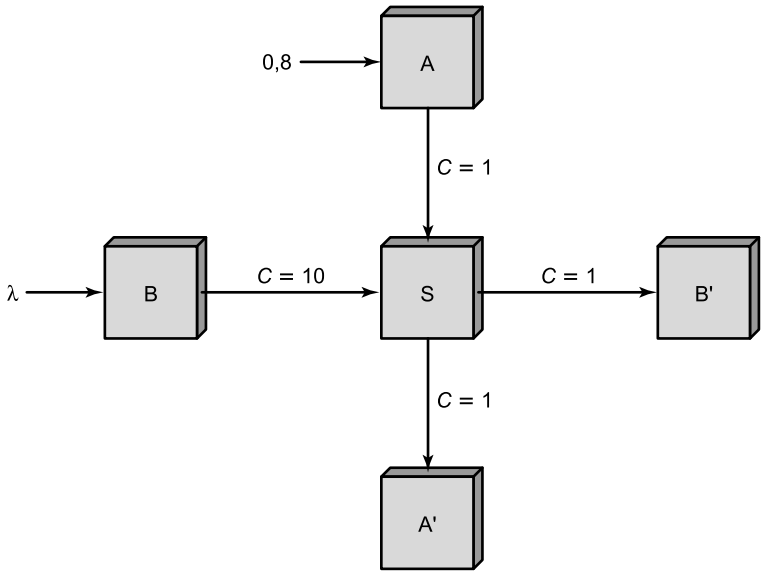


Figura 13.13. Red de nodos.

13.4. Compare la velocidad sostenible de celdas y la tolerancia a la aparición de ráfagas, tal y como se usan en redes ATM, con la tasa de información contratada y el tamaño de ráfaga en exceso, como se usan en redes de retransmisión de tramas. ¿Representan los respectivos términos los mismos conceptos?

13.5. Para que una red de retransmisión de tramas sea capaz de detectar la presencia de congestión e informar posteriormente de ella es necesario que cada manejador de tramas monitorice el comportamiento de sus colas. Si la longitud de las mismas comienza a crecer hasta límites peligrosos, deberían activarse los mecanismos de notificación explícita hacia atrás o hacia adelante, o bien una combinación de ambos, con objeto de intentar reducir el flujo de tramas a través del manejador en cuestión. Éste tiene que elegir el conjunto de conexiones que deberían ser informadas de la congestión, alertando a todas en el caso de que la congestión se vuelva demasiado severa. En las primeras etapas de congestión, el manejador de

tramas podría únicamente notificar a los usuarios cuyas conexiones son las que están generando la mayor parte del tráfico.

En una de las especificaciones de la retransmisión de tramas se sugiere un algoritmo para la supervisión de la longitud de las colas que se muestra en la Figura 13.14. Un ciclo comienza cuando el circuito de salida pasa de estar desocupado (cola vacía) a ocupado (longitud de cola distinta de cero, incluyendo la trama actual). Si se sobrepasa un cierto valor umbral, el circuito se encuentra en un estado de congestión incipiente y los bits de prevención de congestión deberían activarse en algunas o todas las conexiones lógicas que utilizan este circuito. Describa con palabras el funcionamiento del algoritmo y comente sus ventajas.

El algoritmo hace uso de las siguientes variables:

t = Tiempo actual
t_i = Tiempo del i-ésimo evento de llegada o de salida
q_i = Número de tramas en el sistema después del evento
T_0 = Tiempo al comienzo del ciclo anterior
T_1 = Tiempo al comienzo del ciclo actual

El algoritmo consta de tres componentes:

1. Actualizar: empezando con $q_0 := 0$
   Si el i-ésimo evento es un evento de llegada, $q_i := q_{i-1} + 1$
   Si el i-ésimo evento es un evento de salida, $q_i := q_{i-1} - 1$

2.
$$A_{i-1} = \sum_{\substack{i \\ t_i \in [T_0,\ T_1)}} q_{i-1}(t_i - t_{i-1})$$
$$A_i = \sum_{\substack{i \\ t_i \in [T_1,\ t)}} q_{i-1}(t_i - t_{i-1})$$

3.
$$L = \frac{A_i + A_{i-1}}{t - T_0}$$

Figura 13.14. Un algoritmo de retransmisión de tramas.

CAPÍTULO 14

Redes celulares inalámbricas

14.1. Principios de redes celulares
Organización de una red celular
Funcionamiento de sistemas celulares
Efectos de propagación en radio móvil
Desvanecimiento en entornos móviles

14.2. Primera generación analógica
Asignación espectral
Funcionamiento
Canales de control en AMPS

14.3. CDMA de segunda generación
Sistemas celulares de primera y segunda generación
Acceso múltiple por división de código
Consideraciones de diseño de CDMA móvil inalámbrico
IS-95
Enlace de ida en IS-95
Enlace de retorno en IS-95

14.4. Sistemas de tercera generación
Interfaces alternativas
Consideraciones de diseño de CDMA

14.5. Lecturas y sitios web recomendados

14.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- La esencia de una red celular reside en el uso de múltiples transmisores de baja potencia. El área que necesita ser cubierta se divide en celdas siguiendo un patrón hexagonal que proporciona una cobertura total del área.
- Un problema técnico crucial en las redes celulares es el desvanecimiento, problema éste que hace referencia a la variación temporal de la potencia de la señal recibida debido a los cambios existentes en el medio de transmisión o en la trayectoria o trayectorias seguidas.
- Las redes celulares de primera generación fueron analógicas y empleaban multiplexación por división en frecuencia.
- Las redes celulares de segunda generación son digitales. Una técnica de uso ampliamente aceptada es la basada en el acceso múltiple por división de código (CDMA).
- El objetivo de las comunicaciones inalámbricas de tercera generación (3G) es proporcionar comunicaciones inalámbricas de una velocidad suficiente para soportar datos multimedia y vídeo además de voz.

De entre todos los avances espectaculares experimentados en las comunicaciones de datos y las telecomunicaciones, el desarrollo de las redes celulares ha sido, quizá, el que ha tenido un carácter más revolucionario. La tecnología celular es la base de las comunicaciones móviles inalámbricas y posibilita el acceso de usuarios en lugares difícilmente alcanzables por las redes cableadas. La tecnología celular subyace en la telefonía móvil, los sistemas de comunicaciones personales, el acceso inalámbrico a Internet y las aplicaciones web inalámbricas, entre otras.

En este capítulo comenzaremos estudiando los principios básicos utilizados en todas las redes celulares. A continuación, comentaremos tecnologías celulares específicas y estándares que se encuentran convenientemente agrupadas en tres generaciones. La primera generación se basa en una tecnología analógica y, aunque aún sigue siendo utilizada, se puede considerar en fase de extinción. La tecnología dominante hoy en día es la constituida por los sistemas digitales de segunda generación. Finalmente, los sistemas digitales de tercera generación y alta velocidad han comenzado a emerger.

14.1. PRINCIPIOS DE REDES CELULARES

La radio celular es una técnica que fue desarrollada con el fin de incrementar la capacidad disponible para el servicio de telefonía móvil sobre radio. Previamente a la introducción de la radio celular, el servicio de telefonía móvil sobre radio era proporcionado únicamente por un transmisor/receptor de alta potencia. Un sistema típico soportaría en torno a 25 canales con un radio efectivo de alrededor de 80 km. La forma de incrementar la capacidad del sistema es utilizar sistemas de baja potencia con un radio más corto y emplear muchos más transmisores/receptores. Comenzaremos esta sección comentando la organización de los sistemas celulares, examinando más tarde algunos de los detalles de su implementación.

ORGANIZACIÓN DE UNA RED CELULAR

La esencia de una red celular reside en el uso de múltiples transmisores de baja potencia, del orden de 100 W o menos. Dado que el rango de un trasmisor de estas características es pequeño, el área

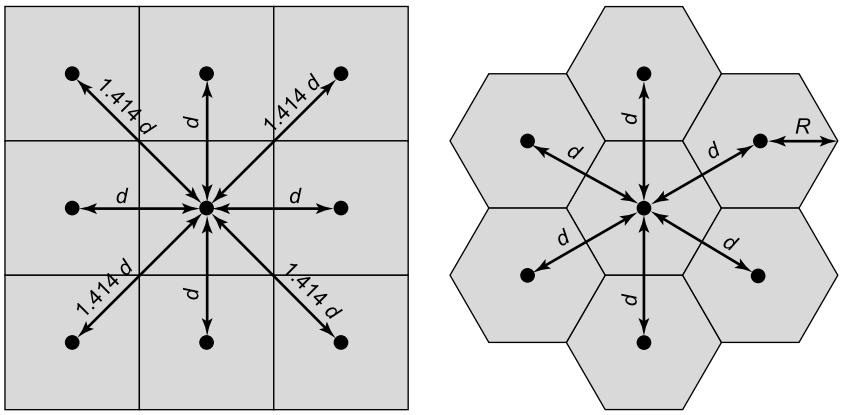


Figura 14.1. Geometrías celulares.

debe ser dividida en celdas, cada una de las cuales dispone de su propia antena. A cada celda se le asigna una banda de frecuencias y una **estación base** (compuesta por un transmisor, un receptor y una unidad de control) que le presta servicio. Las celdas adyacentes reciben una asignación distinta de frecuencias, evitando así la aparición de interferencias o diafonía. No obstante, las celdas suficientemente alejadas entre sí pueden emplear la misma banda de frecuencias.

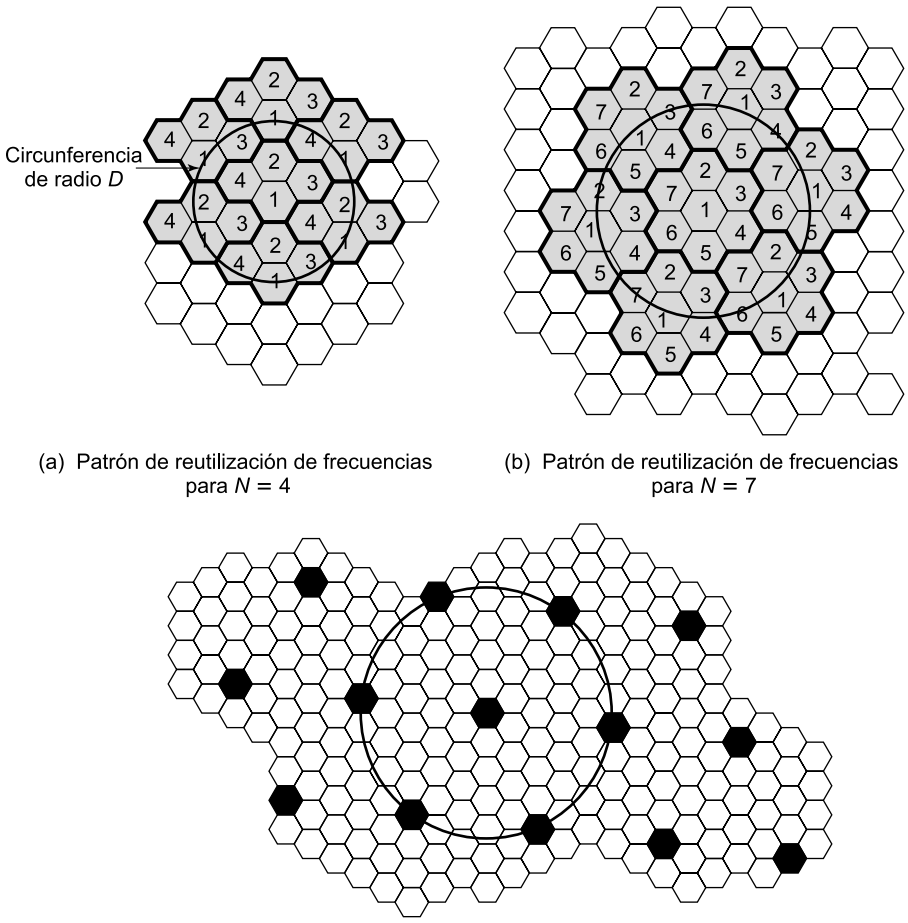
La primera decisión de diseño que se debe tomar es la forma de las celdas que han de cubrir el área. Una matriz de celdas cuadradas sería la disposición más sencilla de definir (*véase* Figura 14.1a). Sin embargo, esta geometría no es la más idónea. Si la anchura de una celda cuadrada es d, cada celda tiene cuatro vecinas a una distancia d y otras cuatro a una distancia $\sqrt{2d}$. A medida que un usuario móvil dentro de una celda se mueva hacia las fronteras de la misma, es deseable que todas las antenas adyacentes estén equidistantes. Esto simplifica la tarea de determinar cuándo cambiar al usuario a una antena adyacente y qué antena seleccionar. Un patrón hexagonal proporciona antenas equidistantes (*véase* Figura 14.1b). El radio de un hexágono se define como el radio de la circunferencia que lo circunscribe (equivalentemente, la distancia desde el centro a cada vértice, que es también igual a la longitud de un lado del hexágono). Para un radio de celda R, la distancia entre el centro de la celda y el centro de cada celda adyacente es $d = \sqrt{3R}$.

En la práctica no se utiliza un patrón hexagonal perfecto. Las alteraciones con respecto a la forma ideal se deben a las limitaciones topográficas, las condiciones locales de propagación de la señal y restricciones para la ubicación de las antenas.

En un sistema celular inalámbrico, el usuario se encuentra limitado en la cantidad de veces que puede utilizar la misma frecuencia para comunicaciones diferentes, dado que las señales, no estando restringidas, pueden interferir con otras incluso si se encuentran geográficamente separadas. Los sistemas que son capaces de soportar un número elevado de comunicaciones simultáneamente precisan de mecanismos para conservar el espectro.

Reutilización de frecuencias

Cada celda en un sistema celular posee un transceptor base. La potencia de transmisión se controla cuidadosamente (hasta el punto que esto sea posible en entornos de comunicaciones con movilidad altamente variable) para permitir la comunicación dentro de la celda utilizando una frecuencia



(a) Patrón de reutilización de frecuencias para $N = 4$

(b) Patrón de reutilización de frecuencias para $N = 7$

(c) Las celdas negras indican una reutilización de frecuencias para $N = 19$

Figura 14.2. Patrones de reutilización de frecuencias.

dada, a la vez que se limita la potencia en esa frecuencia que escapa de los límites de la celda, alcanzando así las adyacentes. El objetivo es usar la misma frecuencia en otras celdas cercanas, permitiendo de esta forma que la misma frecuencia pueda ser empleada en varias conversaciones simultáneamente. Generalmente se asignan entre 10 y 50 frecuencias a cada celda, en función del tráfico esperado.

La cuestión esencial es determinar cuántas celdas debe haber entre dos celdas que utilizan la misma frecuencia para que estas dos no interfieran entre sí. Existen varios patrones de reutilización de frecuencias, algunos de los cuales se ilustran en la Figura 14.2. Si el patrón consta de N celdas y a cada celda se le asigna el mismo número de frecuencias, cada celda puede disponer de K/N frecuencias, donde K es el número total de frecuencias asignadas al sistema. Para AMPS (*véase* Sección 14.2), $K = 395$ y $N = 7$ es el patrón más pequeño que puede proporcionar un aislamiento suficiente entre dos usos de la misma frecuencia. Esto implica que podrá haber, en media, un máximo de 57 frecuencias por celda.

En la caracterización de la reutilización de frecuencias se usan comúnmente los siguientes parámetros:

D = distancia mínima entre los centros de las celdas que utilizan la misma banda de frecuencias (llamados cocanales).

R = radio de la celda.

d = distancia entre los centros de celdas adyacentes ($d = \sqrt{3R}$).

N = número de celdas en cada patrón repetitivo (cada celda en el patrón emplea una banda única de frecuencias), denominado **factor de reutilización**.

En un patrón de celdas hexagonal solamente son posibles los siguientes valores de N:

$$N = I^2 + J^2 + (I \times J),\ I, J = 0, 1, 2, 3, \ldots$$

Los valores posibles de N son, por tanto, 1, 3, 4, 7, 9, 12, 13, 16, 19, 21 y así sucesivamente. Se verifica la relación siguiente:

$$\frac{D}{R} = \sqrt{3N}$$

Esto puede también ser expresado como $D/d = \sqrt{N}$.

Aumento de la capacidad

A medida que más usuarios utilizan el sistema con el tiempo, el tráfico puede crecer hasta el punto de que no haya suficientes frecuencias asignadas a una celda para gestionar sus llamadas. Para hacer frente a esta situación se han utilizado una serie de aproximaciones, entre las cuales citamos las siguientes:

- **Adición de nuevos canales:** cuando un sistema se despliega en una región, lo común es que no todos los canales sean utilizados, de forma que el crecimiento y la expansión pueden ser gestionados ordenadamente mediante la adición de nuevos canales.
- **Uso de frecuencias prestadas:** en el caso más simple, las celdas congestionadas pueden tomar prestadas frecuencias de las celdas adyacentes. Las frecuencias pueden también ser asignadas a las celdas dinámicamente.
- **División de celdas:** la distribución del tráfico y de las características topográficas no son uniformes en la práctica. Este hecho puede utilizarse para conseguir un aumento de la capacidad. Las celdas en zonas de alto uso pueden ser divididas en celdas más pequeñas. Generalmente, las celdas originales tienen un tamaño de entre 6,5 y 13 km, pudiendo ser divididas las más pequeñas. Sin embargo, las celdas de 1,5 km se encuentran cerca del límite práctico de tamaño como solución general (no obstante, véase posteriormente la discusión sobre microceldas). El uso de celdas más pequeñas implica que el nivel de potencia debe ser reducido con objeto de mantener la señal dentro de la celda. Asimismo, a medida que el usuario se mueve cambia de una celda a otra, lo que requiere traspasar la llamada de un transceptor base a otro. Este proceso se denomina *traspaso* (*handoff*). A medida que las celdas son más pequeñas, estos traspasos son más frecuentes. La Figura 14.3 indica esquemáticamente cómo pueden ser divididas las celdas para proporcionar más capacidad. Una reducción del radio en un factor F reduce el área de cobertura e incrementa el número de estaciones base que son necesarias en un factor F^2.
- **Sectorización de celdas:** con esta técnica, una celda se divide en una serie de sectores en forma de cuña, cada uno de los cuales dispone de su propio conjunto de canales. Se emplean

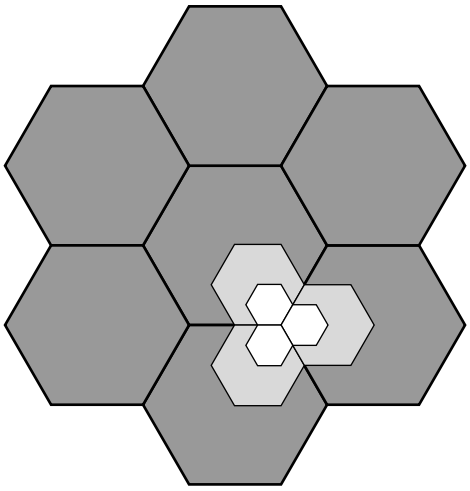


Figura 14.3. División de celdas.

generalmente 3 o 6 sectores por celda, asignándose a cada uno de ellos un subconjunto distinto de los canales de la celda. En la estación base se emplean antenas direccionales enfocadas hacia cada sector.

- **Microceldas:** a medida que las celdas se vuelven más pequeñas, las antenas se desplazan desde lugares como los tejados de edificios altos o colinas hasta puntos de menor altura, como los tejados de edificios más bajos o los laterales de los más altos, e incluso farolas, formando así microceldas. Cada disminución del tamaño de una celda viene acompañada por una reducción de los niveles de potencia radiada de la estación base y de las unidades móviles. Las microceldas son útiles en las calles de las ciudades de zonas congestionadas, a lo largo de las autopistas y dentro de grandes edificios públicos.

En la Tabla 14.1 se sugieren parámetros típicos para las celdas tradicionales, denominadas macroceldas, así como para las microceldas con la tecnología de la que se dispone actualmente. La dispersión del retardo medio de propagación se refiere a la dispersión del retardo de propagación multitrayectoria (es decir, la misma señal sigue diferentes trayectorias y existe un retardo temporal entre la primera y la última recepción de la señal en el receptor). Como se indica, el uso de celdas más pequeñas permite utilizar menor potencia y proporciona condiciones de propagación superiores.

Tabla 14.1. Parámetros típicos para macroceldas y microceldas [ANDE95].

	Macrocelda	**Microcelda**
Radio de la celda	1 a 20 km	0,1 a 1 km
Potencia de transmisión	1 a 10 W	0,1 a 1 W
Variación media del retardo de propagación	0,1 a 10 μs	10 a 100 ns
Velocidad máxima	0,3 Mbps	1 Mbps

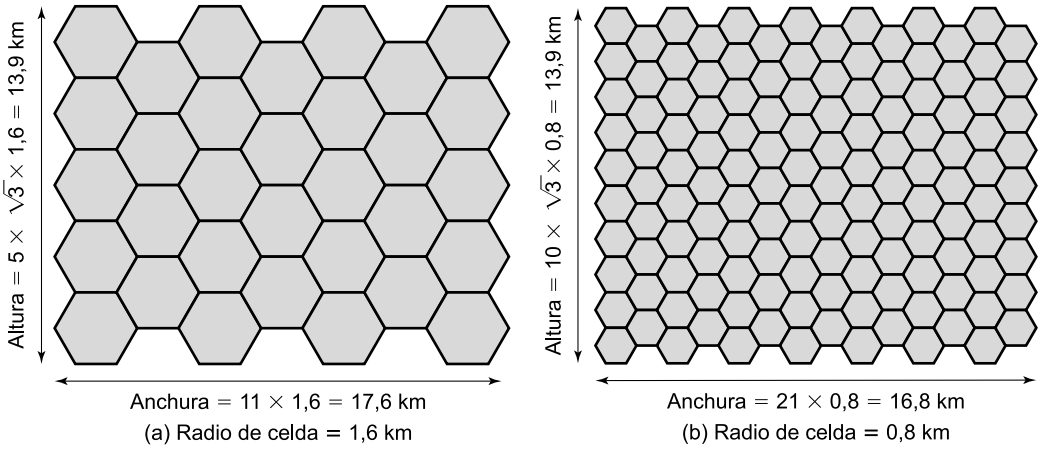


Figura 14.4. Ejemplo de reutilización de frecuencias.

Ejemplo [HAAS00]. Supóngase un sistema de 32 celdas con un radio de celda de 1,6 km, un total de 32 celdas, un ancho de banda en frecuencias que soporta 336 canales de tráfico y un factor de reutilización de $N = 7$. Si existen 32 celdas, ¿qué área geográfica se cubre?, ¿cuántos canales existen por celda? y ¿cuál es el número total de llamadas concurrentes que pueden ser gestionadas? Repítase también para un radio de celda de 0,8 km y 128 celdas.

La Figura 14.4a muestra un patrón aproximadamente hexagonal. El área de un hexágono de radio R es $1{,}5R^2\sqrt{3}$. Un hexágono de radio 1,6 km tiene un área de 6,65 km^2 y el área total cubierta es $6{,}65 \times 32 = 213$ km^2. Para $N = 7$, el número de canales por celda es $336/7 = 48$, con una capacidad total de canales de $48 \times 32 = 1.536$ canales. Para la composición mostrada en la Figura 14.4b, el área cubierta es $1{,}66 \times 128 = 213$ km^2. El número de canales por celda es $336/7 = 48$, con una capacidad total de canales de $48 \times 128 = 6.144$ canales.

FUNCIONAMIENTO DE SISTEMAS CELULARES

La Figura 14.5 muestra los principales elementos de un sistema celular. Aproximadamente en el centro de cada celda se encuentra la estación base (BS, *Base Station*). Cada BS contiene una antena, un controlador y una serie de transceptores para la comunicación sobre los canales asignados a dicha celda. El controlador se usa para gestionar el proceso de llamada entre la unidad móvil y el resto de la red. En un instante dado pueden estar activos una serie de usuarios móviles, moviéndose dentro de la celda y comunicándose con la BS. Cada BS se encuentra conectada con una central de conmutación de telecomunicaciones móviles (MTSO, *Mobile Telecommunications Switching Office*), de tal forma que una MTSO puede prestar servicio a múltiples BS. El enlace entre una MTSO y una BS es normalmente cableado, aunque un enlace inalámbrico es también posible. La MTSO es la responsable de conectar las llamadas entre las unidades móviles y se encuentra también conectada con la red pública de telefonía o telecomunicaciones, de forma que es posible establecer conexiones entre un usuario fijo de la red pública y un usuario móvil en la red celular. La MTSO se encarga de asignar un canal de voz a cada llamada, realizar los traspasos y supervisar las llamadas para obtener la información pertinente para su facturación.

El funcionamiento de un sistema celular se encuentra totalmente automatizado y no precisa de ninguna acción por parte del usuario excepto la realización y recepción de llamadas. Existen dos

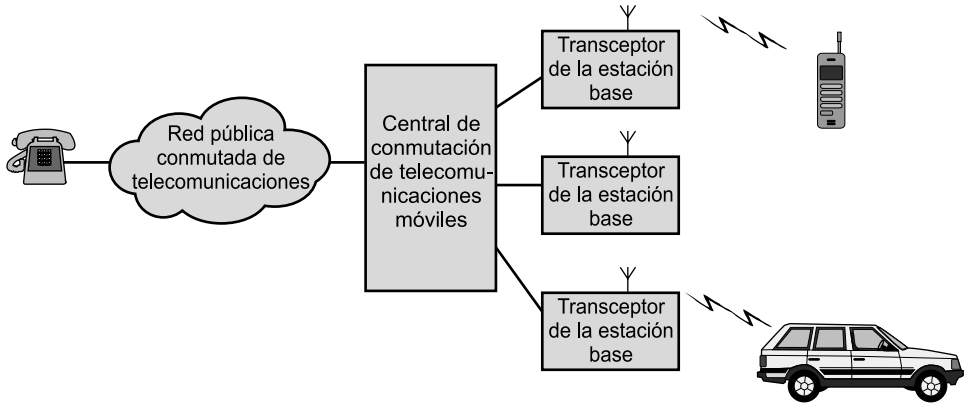

Transceptor de la estación base
Red pública conmutada de telecomunicaciones
Central de conmutación de telecomunicaciones móviles
Transceptor de la estación base
Transceptor de la estación base

Figura 14.5. Estructura general de un sistema celular.

tipos de canales disponibles entre la unidad móvil y la BS: canales de control y canales de tráfico. Los **canales de control** se usan para el intercambio de información concerniente al establecimiento y mantenimiento de las llamadas, así como el establecimiento de una relación entre la unidad móvil y la BS más cercana. Los **canales de tráfico** sustentan la conexión de voz o datos entre los usuarios. La Figura 14.6 ilustra los pasos de una llamada típica entre dos usuarios móviles dentro de una zona controlada por una única MTSO:

- **Inicialización de la unidad móvil:** cuando la unidad móvil es encendida, busca y selecciona el canal de control de establecimiento de mayor potencia (*véase* Figura 14.6a). Las celdas con bandas de frecuencias diferentes difunden periódicamente sobre distintos canales de establecimiento. El receptor selecciona el más potente y lo monitoriza. El efecto de este proceso es que la unidad móvil ha seleccionado automáticamente la antena de la BS de la celda dentro de la cual operará[1]. A continuación tiene lugar, a través de la BS, una etapa de negociación entre la unidad móvil y la MTSO que controla la celda. Mediante esta negociación se identifica al usuario y se registra su localización. Este proceso de rastreo se repite periódicamente mientras que el usuario se encuentre activo con objeto de registrar el movimiento de la unidad. Si ésta entra en una nueva celda, entonces una nueva BS es seleccionada. Adicionalmente, la unidad móvil es supervisada para su localización, punto éste que se discutirá más adelante.

- **Inicio de llamada desde móvil:** una unidad móvil origina una llamada enviando el número de la unidad a la que se llama a través del canal de establecimiento preseleccionado (*véase* Figura 14.6b). El receptor en la unidad móvil comprueba en primer lugar que el canal de establecimiento esté libre examinando la información en el canal de ida (procedente de la BS). Una vez que se detecta libre, la unida móvil puede transmitir sobre el correspondiente canal de retorno (hacia la BS). La BS envía entonces la solicitud hacia la MTSO.

- **Localización:** a continuación, la MTSO intenta completar la conexión con la unidad a la que se llama. Para ello, la MTSO envía un mensaje de localización a ciertas BS en función del número móvil al que se está llamando (*véase* Figura 14.6c). Cada BS transmite la señal de localización en el canal de establecimiento que tiene asignado.

[1] Normalmente, aunque no siempre, la antena y, por tanto, la estación base seleccionada es la más cercana a la unidad móvil. No obstante, éste no es siempre el caso debido a anomalías de propagación.

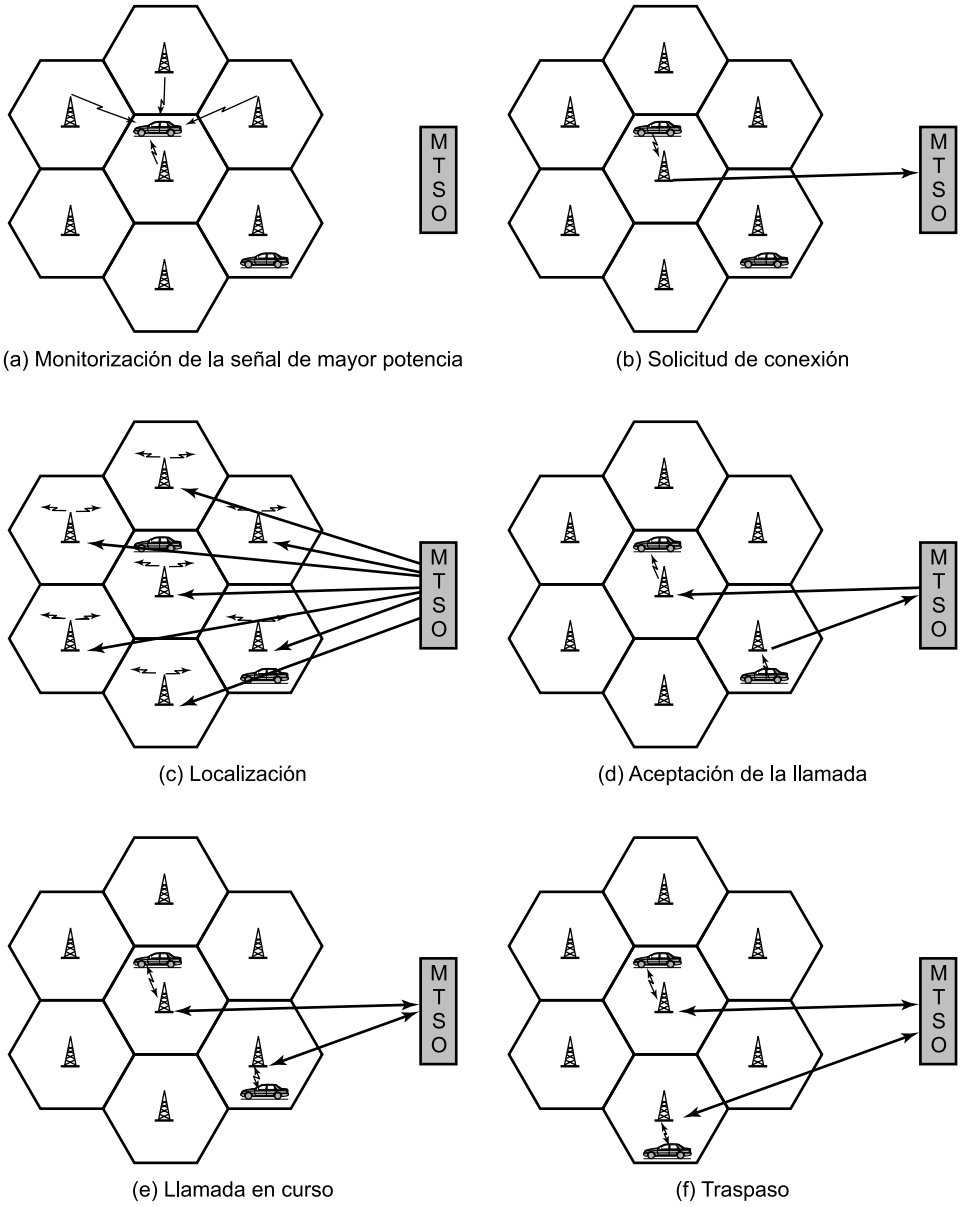


Figura 14.6. Ejemplo de una llamada móvil celular.

- **Aceptación de la llamada:** la unidad móvil llamada reconoce su número en el canal de establecimiento que monitoriza y responde a la BS, la cual envía la respuesta a la MTSO. La MTSO establece un circuito entre la BS que llama y la que recibe la llamada. Al mismo tiempo, la MTSO selecciona un canal de tráfico disponible dentro de la celda de cada BS y notifica a las mismas, las cuales informan a las dos unidades móviles involucradas (*véase* Figura 14.6d). Tras esto, las dos unidades móviles sintonizan los respectivos canales que les han sido asignados.

- **Llamada en curso:** las dos unidades móviles intercambian señales de voz o datos mientras se mantiene la conexión, llevándose a cabo todo el proceso a través de sus respectivas BS y la MTSO (*véase* Figura 14.6c).
- **Traspaso:** si durante la conexión una de las unidades móviles se desplaza fuera del rango cubierto por la celda y entra en la zona de otra, el canal de tráfico tiene que cambiar a otro asignado a la BS en la nueva celda (*véase* Figura 14.6f). El sistema realiza este cambio sin interrumpir la llamada ni alertar al usuario.

Otras funciones que son realizadas por el sistema pero que no se ilustran en la Figura 14.6 son las siguientes:

- **Bloqueo de llamadas:** si todos los canales de tráfico asignados a la BS más cercana se encuentran ocupados durante la etapa de inicio de la llamada, la unidad móvil repite el intento un número de veces preestablecido. Después de un cierto número de intentos fallidos se le devuelve al usuario un tono de ocupado.
- **Terminación de llamadas:** cuando uno de los dos usuarios cuelga, la MTSO recibe una notificación y libera el canal de tráfico entre las dos BS.
- **Corte de llamadas:** debido a interferencias o focos de señal débil en ciertas zonas, es posible que durante una conexión la BS no pueda mantener la potencia de señal mínima requerida durante un determinado periodo de tiempo. En estas situaciones, el canal de tráfico hacia el usuario se corta y la MTSO es informada de este evento.
- **Llamadas hacia/desde usuarios fijos y remotos:** dado que la MTSO se encuentra conectada con la red conmutada pública de telecomunicaciones, puede establecer una conexión entre usuarios móviles en su zona y usuarios fijos a través de la red de telefonía. Más aun, la MTSO puede conectar con otra MTSO remota a través de la red telefónica o mediante líneas dedicadas y establecer una conexión entre un usuario móvil en su zona y otro usuario móvil remoto.

EFECTOS DE PROPAGACIÓN EN RADIO MÓVIL

La comunicación móvil por radio introduce ciertas complejidades que no se encuentran en las comunicaciones por cable o en las comunicaciones inalámbricas fijas. Dos problemas fundamentales son los que tienen que ver con la potencia de la señal y los efectos de la propagación de la misma.

- **Potencia de la señal:** la potencia de la señal entre la BS y la unidad móvil debe ser lo suficientemente fuerte para mantener la calidad de la señal en la recepción, sin llegar a interferir demasiado con canales de otras celdas que estén utilizando la misma banda de frecuencias. Existen numerosos factores que complican este fenómeno. El ruido de origen humano varía considerablemente, resultando en niveles de ruido variables. Por ejemplo, el ruido de encendido de los coches en el rango de las frecuencias que se utilizan en sistemas celulares es mayor en las ciudades que en zonas suburbanas. Otras fuentes de señal cambian de un lugar a otro. La potencia de la señal varía como una función de la distancia entre la BS y cualquier punto dentro de su celda. Además, la potencia de la señal varía dinámicamente a medida que la unidad móvil se desplaza.
- **Desvanecimiento:** incluso si la potencia de la señal se encuentra dentro de un rango efectivo, los efectos de propagación pueden interrumpir la señal y ocasionar errores. El desvanecimiento se comenta posteriormente en esta sección.

En el diseño de una distribución de celdas, el ingeniero de comunicaciones debe tener en consideración estos efectos de propagación, así como el nivel máximo deseado de potencia de transmisión en la BS y las unidades móviles, la altura típica de la antena de una unidad móvil y la altura disponible para la antena de la BS. Todos estos factores determinarán el tamaño de cada celda individual. Desafortunadamente, y como acabamos de comentar, los efectos de propagación son dinámicos y difíciles de predecir. Lo mejor que puede hacerse es proponer un modelo basándose en datos empíricos y aplicarlo a un entorno dado para obtener ciertas pautas sobre el tamaño de la celda. Uno de los modelos más ampliamente utilizados fue desarrollado por Okumura et al. [OKUM68] y posteriormente refinado por Hata [HATA80]. El original consistía en un análisis detallado de la zona de Tokio y generaba información sobre las pérdidas en cada trayectoria dentro de un entorno urbano. El modelo de Hata es una formulación empírica que tiene en consideración todo un abanico de entornos y condiciones. Para un entorno urbano, la pérdida predicha en la trayectoria es:

$$L_{\text{dB}} = 69{,}55 + 26{,}16 \log f_c - 13{,}82 \log h_t - A(h_r) + (44{,}9 - 6{,}55 \log h_t) \log d \qquad (14.1)$$

donde

f_c = frecuencia de la portadora en MHz desde 150 hasta 1.500 MHz.

h_t = altura de la antena emisora (estación base) en m, desde 30 hasta 300 m.

h_r = altura de la antena receptora (estación móvil) en m, desde 1 hasta 10 m.

d = distancia de propagación entre las antenas en km, de 1 a 20 km.

$A(h_r)$ = factor de corrección para la altura de la antena móvil.

Para el caso de una ciudad pequeña o mediana, el factor de corrección viene dado por

$$A(h_r) = (1{,}1 \log f_c - 0{,}7)h_r - (1{,}56 \log f_c - 0{,}8) \text{ dB}$$

El factor de corrección para ciudades grandes es

$$A(h_r) = 8{,}29[\log (1{,}54h_r)]^2 - 1{,}1 \text{ dB} \quad \text{para } f_c \leqslant 300 \text{ MHz}$$

$$A(h_r) = 3{,}2[\log(11{,}75h_r)]^2 - 4{,}97 \text{ dB} \quad \text{para } f_c \geqslant 300 \text{ MHz}$$

Para estimar la pérdida en la trayectoria en un área suburbana, la expresión utilizada en la Ecuación (14.1) para entornos urbanos es modificada como se muestra a continuación

$$L_{\text{dB}}(\text{suburbano}) = L_{\text{dB}}(\text{urbano}) - 2[\log (f_c/28)]^2 - 5{,}4$$

Para el caso de la estimación de la pérdida en zonas abiertas, la expresión se modifica de la siguiente forma:

$$L_{\text{dB}}(\text{abierto}) = L_{\text{dB}}(\text{urbano}) - 4{,}78(\log f_c)^2 - 18{,}733(\log f_c) - 40{,}98$$

El modelo de Okumura/Hata está considerado como uno de los mejores en términos de precisión en la predicción de la pérdida de propagación, a la vez que proporciona una forma práctica de estimar dicha pérdida en una amplia variedad de situaciones [FREE97, RAPP97].

Ejemplo [FREE97]. Sea $f_c = 900$ MHz, $h_t = 40$ m, $h_r = 5$ m y $d = 10$ km. Estímese la pérdida en la trayectoria para una ciudad de tamaño medio.

$$A(h_r) = (1{,}1 \log 900 - 0{,}7)5 - (1{,}56 \log 900 - 0{,}8) \text{ dB}$$
$$= 12{,}75 - 3{,}8 = 8{,}95 \text{ dB}$$

$$L_{\text{dB}} = 69{,}55 + 26{,}16 \log 900 - 13{,}82 \log 40 - 8{,}95$$
$$+ (44{,}9 - 6{,}55 \log 40) \log 10$$
$$= 69{,}55 + 77{,}28 - 22{,}14 - 8{,}95 + 34{,}4 = 150{,}14 \text{ dB}$$

DESVANECIMIENTO EN ENTORNOS MÓVILES

Quizá el problema más desafiante desde un punto de vista técnico al que se enfrentan los ingenieros de sistemas de comunicaciones es el del desvanecimiento en un entorno móvil. El término *desvanecimiento* se refiere a la variación temporal de la potencia de la señal recibida causada por cambios en el medio de transmisión o en la trayectoria o trayectorias. En un entorno fijo, el desvanecimiento se debe a cambios en las condiciones atmosféricas, como la lluvia. Pero en un entorno móvil, donde una de las dos antenas se desplaza con respecto a la otra, la presencia de obstáculos cambia a lo largo del tiempo, creando así efectos de transmisión complejos.

Propagación multitrayectoria

Existen tres mecanismos de propagación que intervienen en el problema y que son ilustrados en la Figura 14.7. La **reflexión** ocurre cuando una señal electromagnética alcanza una superficie que es relativamente grande en comparación con la longitud de onda de la señal. Supongamos, por ejemplo, que se recibe una onda reflejada en la tierra y cercana a la unidad móvil. Dado que dicha onda posee un desplazamiento de fase de 180º tras la reflexión, la onda en la línea visual (LOS, *Line Of Sight*) y la onda reflejada tenderán a cancelarse, ocasionando una alta pérdida de señal[2]. Además, aparecen interferencias multitrayectoria puesto que la antena móvil se encuentra a menor altura que la mayor parte de las estructuras artificiales en la zona. Estas ondas reflejadas pueden interferir constructivamente o destructivamente en el receptor.

La **difracción** aparece en el vértice de un cuerpo impenetrable cuyo tamaño es significativamente superior a la longitud de onda de la onda de radio. Cuando una onda de radio se encuentra con tal vértice, las ondas se propagan en diferentes direcciones con el vértice como fuente. Así, las señales pueden ser recibidas incluso cuando no existe una LOS libre de obstáculos desde el transmisor.

La **dispersión** aparece si el tamaño de un obstáculo es del orden de la longitud de onda de la señal o menor, ocasionando que la señal se disperse en varias señales más débiles. Existen varios objetos que pueden producir dispersión a las frecuencias de microondas típicas que se usan en redes celulares, como las farolas o las señales de tráfico. Esto hace que los efectos de dispersión sean difíciles de predecir.

[2] Por otro lado, la señal reflejada recorre un camino más largo, lo cual ocasiona un desplazamiento de fase debido al retardo relativo a la señal no reflejada. Cuando este retardo es equivalente a la mitad de la longitud de onda, las dos señales vuelven a poseer la misma fase.

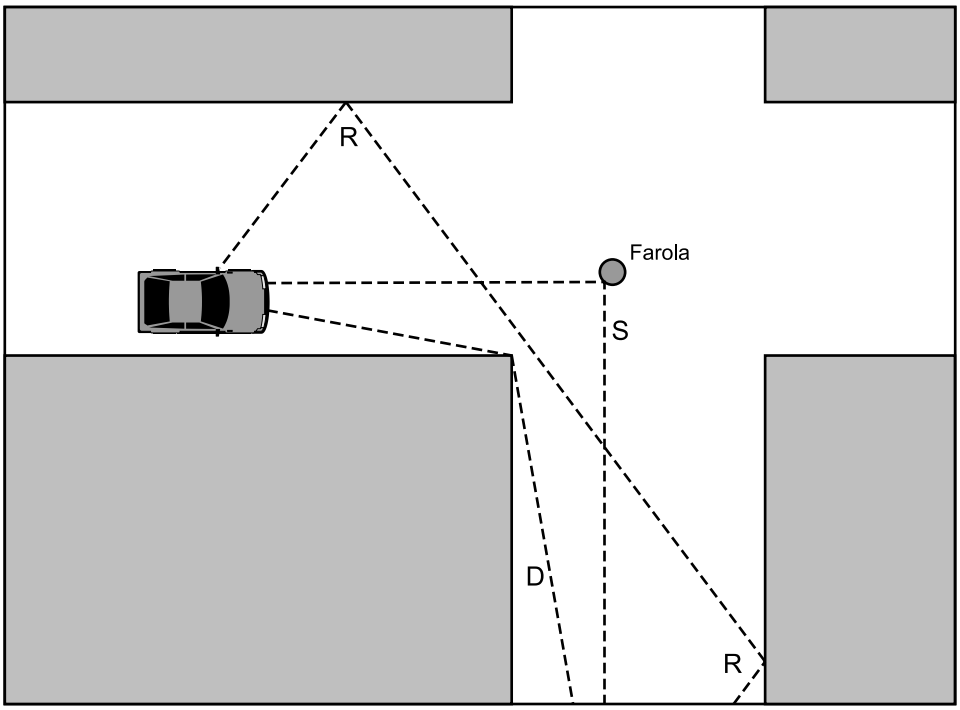


Figura 14.7. Ilustración de los tres mecanismos de propagación importantes: reflexión (R), dispersión (S) y difracción (D) [ANDE95].

Los tres efectos de propagación mencionados influyen en el rendimiento del sistema de varias formas, dependiendo de las condiciones locales y a medida que la estación móvil se desplaza dentro de una celda. Generalmente, tanto la difracción como la dispersión son efectos menores cuando la unidad móvil posee una LOS clara hacia el transmisor, aunque la reflexión puede alcanzar un impacto significativo. Si no existe una LOS clara, tal y como sucede en las calles de una zona urbana, entonces la difracción y la dispersión son las principales fuentes de problemas de recepción de la señal.

Efectos de la propagación multitrayectoria

Como acabamos de observar, uno de los efectos indeseables de la propagación multitrayectoria es que múltiples copias de una señal pueden ser recibidas con diferentes fases. Si estas fases se suman destructivamente, el nivel de la señal con respecto al ruido disminuye, haciendo más difícil la detección de la señal en el receptor.

Un segundo fenómeno de particular importancia para la transmisión digital es la interferencia intersimbólica (ISI, *Intersymbol Interference*). Supongamos que se envía un pulso estrecho a una determinada frecuencia a través de un enlace entre una antena fija y una unidad móvil. En la Figura 14.8 se muestra lo que el canal puede entregar al receptor si el impulso es enviado en dos instantes de tiempo distintos. La línea superior muestra los dos pulsos en el momento de ser transmitidos, mientras que en la inferior se hace lo propio con los pulsos resultantes en el receptor. En cada caso, el primer pulso recibido es la señal LOS deseada. Su magnitud puede cambiar debido a alteraciones en la atenuación atmosférica. Adicionalmente, la pérdida de la señal LOS se

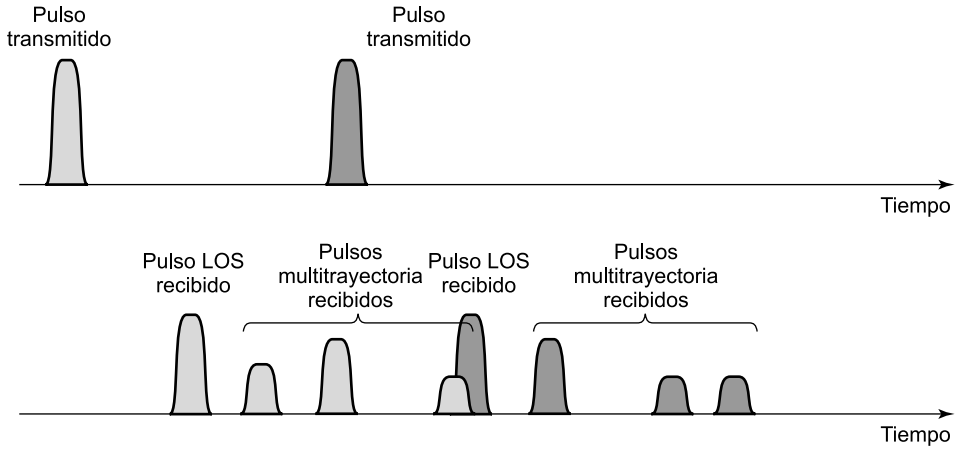


Figura 14.8. Dos pulsos en una multitrayectoria variable en el tiempo.

incrementa a medida que la unidad móvil se desplaza alejándose de la antena fija. Pero, además de este pulso primario, pueden aparecer múltiples pulsos secundarios debidos a la reflexión, difracción y dispersión. Supóngase ahora que el pulso codifica uno o más bits de datos. En ese caso, una o más copias retardadas del pulso pueden llegar al receptor al mismo tiempo que el pulso primario de un bit posterior, actuando como una forma de ruido frente a él y haciendo la recuperación de la información del bit más difícil.

La localización de los obstáculos cambia a medida que la antena móvil se desplaza, ocasionando que el número, magnitud y localización temporal de los pulsos secundarios también cambie. Esto dificulta el diseño de técnicas de procesamiento de la señal que filtren los efectos de la propagación multitrayectoria de tal forma que la señal deseada sea recuperada con fidelidad.

Tipos de desvanecimientos

Los efectos de desvanecimiento en un entorno móvil pueden ser clasificados como rápidos o lentos. Volviendo a la Figura 14.7, a medida que la unidad móvil se desplaza a lo largo de una calle en una zona urbana, aparecen variaciones rápidas de la potencia de la señal en distancias de alrededor de la mitad de la longitud de onda. A una frecuencia de 900 MHz, que es típica para aplicaciones móviles celulares, la longitud de onda es de 0,33 m. Los cambios de amplitud pueden llegar a ser de 20 o 30 dB en una distancia corta. Este tipo de fenómeno de desvanecimiento que ocasiona un cambio tan brusco, conocido como **desvanecimiento rápido**, afecta no sólo a los teléfonos móviles en automóviles, sino también a un usuario con un teléfono móvil caminando por la calle.

El entorno urbano cambia a medida que el usuario móvil recorre distancias superiores a la de la longitud de onda, moviéndose alrededor de edificios de diferentes alturas, zonas descubiertas, intersecciones, etc. A lo largo de estas distancias más largas, existe un cambio en el nivel de potencia media recibida sobre el cual se producen las fluctuaciones rápidas. A este cambio se le denomina **desvanecimiento lento**.

Alternativamente, los efectos de desvanecimiento pueden clasificarse como planos o selectivos. El **desvanecimiento plano**, también denominado no selectivo, es un tipo de desvanecimiento en el que todas las componentes en frecuencia de la señal recibida fluctúan en la misma proporción simultáneamente. El **desvanecimiento selectivo** afecta desigualmente a las distintas componentes

espectrales de una señal de radio. Usualmente, el término *desvanecimiento selectivo* es sólo significativo en comparación con el ancho de banda de todo el canal de comunicaciones. Si se produce una atenuación de una porción del ancho de banda de la señal, el desvanecimiento se considera selectivo; el desvanecimiento no selectivo implica que el ancho de banda de interés de la señal es más estrecho que el espectro afectado por el desvanecimiento y que se encuentra completamente cubierto por éste.

Mecanismos de compensación de errores

Los esfuerzos para compensar los diversos errores y distorsiones introducidos por el desvanecimiento multitrayectoria se pueden agrupar en tres categorías generales: corrección de errores hacia adelante, ecualización adaptativa y técnicas de diversidad. En un entorno móvil inalámbrico típico se combinan técnicas de las tres clases para combatir las tasas de errores que aparecen.

La **corrección de errores hacia adelante** se emplea en aplicaciones de transmisión digital: aquellas en las cuales las señales transmitidas transportan datos o voz o vídeo digitalizados. En aplicaciones móviles inalámbricas, la razón entre el número de bits totales enviados frente a los bits de datos enviados se encuentra generalmente entre 2 y 3. Esto puede parecer una cantidad excesiva de información de sobrecarga, puesto que la capacidad del sistema se limita a la mitad o una tercera parte de su potencial, pero los entornos móviles inalámbricos presentan unos índices de dificultad tales que estos niveles de redundancia son necesarios. En el Capítulo 6 se discuten las técnicas de corrección de errores hacia adelante.

La **ecualización adaptativa** puede aplicarse a las transmisiones que transportan información analógica (por ejemplo, voz o vídeo analógico) o información digital (por ejemplo, datos digitales o voz o vídeo digitalizado) y es utilizado para combatir la interferencia intersimbólica. El proceso de ecualización involucra algún método para reunir la energía dispersada de los símbolos y agruparla en torno al intervalo de tiempo correspondiente. La ecualización es un tema muy amplio y las técnicas que se emplean van desde el uso de los denominados circuitos analógicos de nudos hasta sofisticados algoritmos de procesamiento digital de señales.

La **diversidad** está basada en el hecho de que los canales individuales experimentan fenómenos de desvanecimiento independientes. Es posible, por tanto, compensar los efectos de error proporcionando de alguna forma múltiples canales lógicos entre el emisor y el receptor y enviando una parte de la señal sobre cada uno de ellos. Esta técnica no elimina los errores, sino que reduce la tasa de los mismos dispersando la transmisión para evitar que se vea sometida a la mayor tasa de errores que se pudiera producir. Las otras técnicas (ecualización y corrección de errores hacia adelante) pueden entonces hacer frente a la tasa de errores reducida.

Algunas técnicas de diversidad involucran al camino físico de la transmisión y son denominadas de **diversidad espacial**. Por ejemplo, una serie de antenas cercanas pueden ser utilizadas para recibir el mensaje, combinando las señales de alguna forma para reconstruir la señal más probable. Otro ejemplo es el uso de múltiples antenas direccionales ubicadas en el mismo punto, cada una orientada hacia un ángulo de recepción diferente, también con las señales combinadas para reconstruir la señal transmitida.

El término *diversidad* se utiliza más comúnmente para referirse a las técnicas de diversidad en frecuencia o en tiempo. En las técnicas de **diversidad en frecuencia**, la señal se disemina sobre un ancho de banda mayor o bien se transporta sobre varias portadoras a diferentes frecuencias. El ejemplo más importante de este enfoque es el espectro expandido, que se discute en el Capítulo 9.

14.2. PRIMERA GENERACIÓN ANALÓGICA

Las redes celulares telefónicas originales, a las que hoy nos referimos como sistemas de primera generación, proporcionaban canales analógicos de tráfico. Desde principios de 1980, el sistema de primera generación más común en Norteamérica ha sido el **Servicio Avanzado de Telefonía Móvil** (AMPS, *Advanced Mobile Phone Service*), desarrollado por AT&T. Este enfoque es habitual también en Sudamérica, Australia y China y, aunque está siendo gradualmente sustituido por los sistemas de segunda generación, AMPS todavía se utiliza. En esta sección se describe brevemente AMPS.

ASIGNACIÓN ESPECTRAL

En Norteamérica están reservadas dos bandas de 25 MHz para AMPS (*véase* Tabla 14.2), una para la transmisión desde la estación base hacia la unidad móvil (869-894 MHz) y otra para la transmisión desde la unidad móvil hacia la estación base (824-849 MHz). Cada una de estas bandas está dividida en dos para fomentar la competencia (es decir, de forma tal que puedan ser ubicados dos operadores). Así, a cada operador se le asignan únicamente 12,5 MHz en cada dirección para su sistema. Los canales se encuentran espaciados entre sí 30 kHz, lo que permite un total de 416 canales por operador. Están asignados 21 canales para control, de forma que quedan 395 canales para el transporte de llamadas. Los canales de control son canales de datos que funcionan a 10 kbps. Por otra parte, los canales de voz transportan la conversación en analógico utilizando modulación en frecuencia. La información de control se envía también sobre los canales de voz como datos en ráfagas. Dado que este número de canales no es adecuado para la mayor parte de los mercados, se hace necesario encontrar alguna forma de utilizar menos ancho de banda por conversación o bien reutilizar frecuencias. Ambas aproximaciones han sido utilizadas en las distintas aproximaciones a la telefonía móvil, siendo la reutilización de frecuencias la técnica empleada en el caso de AMPS.

Tabla 14.2. Parámetros de AMPS.

Banda de transmisión de la estación base	869 a 894 MHz
Banda de transmisión de la unidad móvil	824 a 849 MHz
Espaciado entre los canales de ida y de retorno	45 MHz
Ancho de banda de cada canal	30 kHz
Número de canales de voz full-duplex	790
Número de canales de control full-duplex	42
Potencia máxima de la unidad móvil	3 vatios
Tamaño de celda (radio)	2 a 20 km
Modulación, canal de voz	FM, 12 kHz de desviación de pico
Modulación, canal de control	FSK, 8 kHz de desviación de pico
Tasa de transmisión de datos	10 kbps
Código de control de errores	BCH (48, 36, 5) y (40, 28, 5)

FUNCIONAMIENTO

Cada teléfono celular compatible con AMPS incluye un *módulo de asignación de número* (NAM, *Numeric Assignment Module*) en una memoria de sólo lectura. El NAM contiene el número de teléfono del terminal asignado por el proveedor del servicio, así como el número de serie asignado por el fabricante. Cuando se enciende el teléfono, éste envía su número de serie y su número de teléfono hacia la MTSO (*véase* Figura 14.5). La MTSO mantiene una base de datos con información sobre las unidades móviles que han sido declaradas robadas y utiliza los números de serie para bloquear dichas unidades. Por otro lado, la MTSO utiliza el número de teléfono para gestionar la facturación. Si el teléfono está siendo utilizado en una ciudad remota, el coste del servicio es cargado al proveedor local del usuario.

Cuando tiene lugar una llamada se produce la siguiente secuencia de eventos [COUC01]:

1. El abonado inicia la llamada tecleando el número de teléfono destino y pulsando la tecla de envío.
2. La MTSO verifica que el número de teléfono es válido y que el usuario dispone de autorización para realizar la llamada. Algunos proveedores de servicios requieren que el usuario introduzca un número de identificación personal (PIN, *Personal Identification Number*) además del número de teléfono a llamar para verificar que el teléfono no ha sido robado.
3. La MTSO envía un mensaje al teléfono celular del usuario indicándole los canales de tráfico que se usarán para el envío y la recepción.
4. La MTSO envía una señal de llamada al usuario llamado. Todas estas operaciones (pasos del 2 al 4) ocurren dentro de los 10 s posteriores al inicio de la llamada.
5. Cuando la parte llamada responde, la MTSO establece un circuito entre las dos partes involucradas y comienza a registrar la información pertinente para la facturación.
6. Cuando una de las partes cuelga, la MTSO libera el circuito y los canales de radio y finaliza el registro de información de facturación.

CANALES DE CONTROL EN AMPS

Cada servicio AMPS incluye 21 canales de control *full-duplex* de 30 kHz, consistentes en 21 canales de control de retorno (RCC, *Reverse Control Channels*) desde el abonado hacia la estación base y 21 canales de ida desde la estación base al abonado. Estos canales transmiten datos digitales usando FSK, enviándose éstos en tramas en ambos tipos de canales.

La información de control puede transmitirse sobre un canal de voz durante una conversación en curso. La unidad móvil o la estación base pueden insertar una ráfaga de datos desconectando la transmisión FM de voz durante unos 100 ms y reemplazándola por un mensaje codificado con FSK. Estos mensajes son utilizados para el intercambio de información urgente, como cambios en el nivel de potencia y traspasos.

14.3. CDMA DE SEGUNDA GENERACIÓN

Esta sección comienza comentando algunas líneas generales para pasar a continuación a examinar en detalle un tipo de sistema celular de segunda generación.

SISTEMAS CELULARES DE PRIMERA Y SEGUNDA GENERACIÓN

Las redes celulares de primera generación, como AMPS, se volvieron populares tan rápidamente que surgió la amenaza de saturarse la capacidad disponible del sistema. Los sistemas de segunda generación han sido desarrollados para proporcionar señales de una calidad superior, con mayor velocidad de datos para soportar servicios digitales y una mayor capacidad. En [BLAC99b] se enumeran los siguientes puntos como diferencias clave entre las dos generaciones:

- **Canales de tráfico digitales:** la diferencia más notable entre las dos generaciones es que, mientras que los sistemas de primera generación son casi puramente analógicos, los de segunda son digitales. En concreto, los sistemas de primera generación están diseñados para soportar canales de voz usando FM; el tráfico digital se soporta únicamente mediante el uso de un módem que convierte los datos digitales a una forma analógica. Los sistemas de segunda generación proporcionan canales digitales de tráfico que soportan directamente los datos digitales. El tráfico de voz es codificado en forma digital previamente a su transmisión. Por supuesto, en los sistemas de segunda generación, el tráfico de usuario (voz o datos) debe ser convertido a una señal analógica para su transmisión entre la unidad móvil y la estación base (por ejemplo, *véase* la Figura 5.15).
- **Cifrado:** debido a que todo el tráfico del usuario, así como el tráfico de control, está digitalizado en los sistemas de segunda generación, es una cuestión relativamente simple su cifrado para prevenir las escuchas clandestinas. Todos los sistemas de segunda generación proporcionan esta capacidad, al contrario que los de primera generación que envían el tráfico en claro, sin seguridad alguna.
- **Detección y corrección de errores:** el flujo de tráfico digital en sistemas de segunda generación se presta al uso de técnicas de detección y corrección de errores como las descritas en el Capítulo 6. El resultado puede ser una recepción muy clara de la voz.
- **Acceso a los canales:** en los sistemas de primera generación, cada celda soporta un número de canales. En un instante de tiempo determinado, un canal es asignado únicamente a un usuario. Los sistemas de segunda generación proporcionan de igual forma varios canales por celda, pero cada canal se comparte dinámicamente por un número de usuarios mediante el uso de acceso múltiple por división en el tiempo (TDMA) o acceso múltiple por división de código (CDMA). En esta sección describiremos los sistemas basados en CDMA.

A partir de 1990 se han desarrollado y desplegado diferentes sistemas de segunda generación. Un buen ejemplo lo constituye el esquema IS-95 usando CDMA.

ACCESO MÚLTIPLE POR DIVISIÓN DE CÓDIGO

El uso de CDMA para sistemas celulares se puede describir como sigue. Al igual que con FDMA, a cada celda se le asigna una banda de frecuencias que es dividida en dos partes, la mitad para el retorno (unidad móvil a estación base) y la otra mitad para la ida (estación base a unidad móvil). Para comunicaciones *full-duplex*, una unidad móvil utiliza tanto el canal de ida como el de retorno. La transmisión se produce en la forma de espectro expandido de secuencia directa (DS-SS, *Direct-Sequence Spread Spectrum*), el cual utiliza un código de minibits (*chips*) para incrementar la velocidad de datos de la transmisión, resultando en un ancho de banda aumentado para la señal. El acceso múltiple se consigue asignando códigos de minibits ortogonales a los distintos usuarios, de tal forma que el receptor puede recuperar la transmisión de una unidad individual a partir de varias transmisiones.

CDMA presenta una serie de ventajas para su uso en una red celular:

- **Diversificación de frecuencias:** puesto que la transmisión es expandida sobre un ancho de banda amplio, los factores dependientes de la frecuencia que perjudican la transmisión, como las ráfagas de ruido y el desvanecimiento selectivo, ocasionan un efecto menor en la señal.
- **Resistencia multitrayectoria:** además de la capacidad de DS-SS para combatir el desvanecimiento multitrayectoria mediante la diversificación de frecuencias, los códigos de minibits utilizados para CDMA no sólo exhiben una baja correlación cruzada sino también una baja autocorrelación. Por tanto, una versión de la señal retardada en más del intervalo de un *chip* no interfiere con la señal dominante tanto como en otros entornos multitrayectoria.
- **Privacidad:** la privacidad es inherente dado que el espectro expandido se obtiene mediante señales del tipo del ruido, poseyendo cada usuario un código único.
- **Degradación ordenada:** con el uso de FDMA o TDMA, un número fijo de usuarios pueden acceder al sistema simultáneamente. Con CDMA, sin embargo, a medida que más usuarios acceden al sistema a la vez, el nivel de ruido y, por tanto, la tasa de errores, se incrementa; el sistema se degrada siempre gradualmente hasta el punto en que la tasa de errores es inaceptable.

Dos inconvenientes del uso celular de CDMA deben también mencionarse:

- **Autointerferencias:** a no ser que todos los usuarios móviles se encuentren perfectamente sincronizados, las transmisiones que se reciben procedentes de diferentes usuarios no estarán perfectamente alineadas en cuanto a las fronteras de los códigos de minibits. Así, las secuencias expandidas de los distintos usuarios no serán ortogonales y existirá cierto nivel de correlación cruzada. Éste no es el caso de TDMA o FDMA, en los que las señales recibidas son ortogonales (o casi) si se emplean bandas razonables de protección en tiempo o frecuencia, respectivamente.
- **El problema cerca-lejos:** las señales cercanas al receptor se reciben con menor atenuación que las señales lejanas. Dada la ausencia de una ortogonalidad completa, las transmisiones procedentes de las estaciones móviles más lejanas pueden ser más difíciles de recibir.

CONSIDERACIONES DE DISEÑO DE CDMA MÓVIL INALÁMBRICO

Antes de entrar en detalle con el ejemplo de IS-95, resulta útil considerar algunos aspectos generales sobre el diseño de un sistema celular CDMA.

El receptor RAKE

En un entorno de propagación multitrayectoria, como es el caso común de los sistemas celulares, si las múltiples versiones de una señal alcanzan más de un intervalo de minibit diferente, el receptor puede recuperar la señal correlacionando la secuencia del minibit con la señal dominante recibida, otorgando al resto de señales el tratamiento de ruido. No obstante, es posible obtener un rendimiento superior si el receptor intenta recuperar las señales procedentes de diferentes trayectorias, con retardos aceptables, y combinarlas apropiadamente. Este principio es el empleado en el receptor RAKE.

La Figura 14.9 ilustra el principio de funcionamiento del receptor RAKE. La señal binaria original que va a ser transmitida es expandida utilizando la operación lógica O-exclusivo (XOR) con

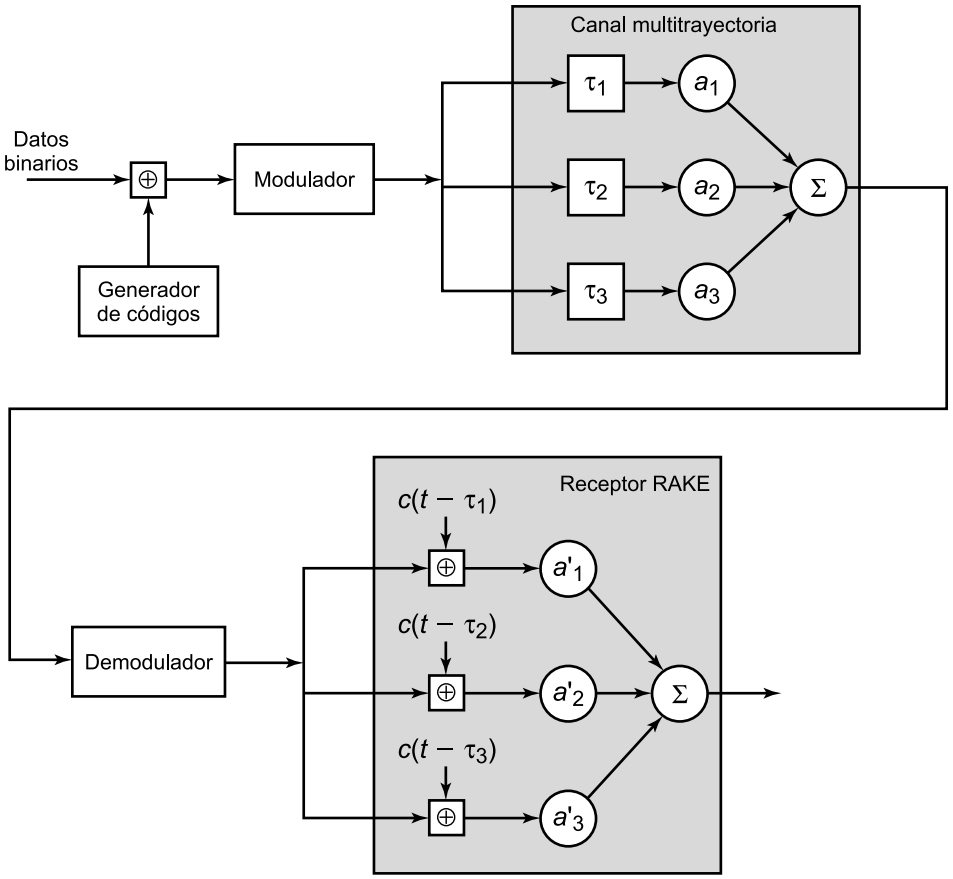


Figura 14.9. Principio de funcionamiento del receptor RAKE [PRAS98].

el código de *chips* del transmisor. La secuencia expandida se modula entonces para su transmisión sobre el canal inalámbrico. Debido a los efectos de la propagación multitrayectoria, el canal genera múltiples copias de la señal, cada una con un retardo temporal diferente (τ_1, τ_2, etc.) y un factor de atenuación distinto (a_1, a_2, etc.). En el receptor se demodulan las señales combinadas. El flujo de códigos se inyecta entonces en varios correladores, cada uno retardado en una cantidad de tiempo distinta. Las señales resultantes se combinan utilizando los factores de ponderación estimados para el canal.

IS-95

El esquema CDMA de segunda generación más ampliamente utilizado es el IS-95, que se encuentra desplegado principalmente en Norteamérica. Las estructuras de transmisión sobre los enlaces de ida y retorno son diferentes y se describen separadamente.

ENLACE DE IDA EN IS-95

En la Tabla 14.3 se listan los parámetros del enlace del canal de ida. El enlace de ida se compone de hasta 64 canales lógicos CDMA, cada uno ocupando el mismo ancho de banda de 1.228 kHz (*véase* Figura 14.10a). Éste soporta cuatro tipos de canales:

Tabla 14.3. Parámetros de canal para el enlace de ida en IS-95.

Canal	Sincroni-zación	Localización		Conjunto de velocidades de tráfico 1				Conjunto de velocidades de tráfico 2			
Tasa de datos (bps)	1.200	4.800	9.600	1.200	2.400	4.800	9.600	1.800	3.600	7.200	14.400
Repetición de código	2	2	1	8	4	2	1	8	4	2	1
Tasa de modulación de símbolos (sps)	4.800	19.200	19.200	19.200	19.200	19.200	19.200	19.200	19.200	19.200	19.200
Minibits PN/símbolo de modulación	256	64	64	64	64	64	64	64	64	64	64
Minibits PN/bit	1.024	256	128	1.024	512	256	128	682,67	341,33	170,67	85,33

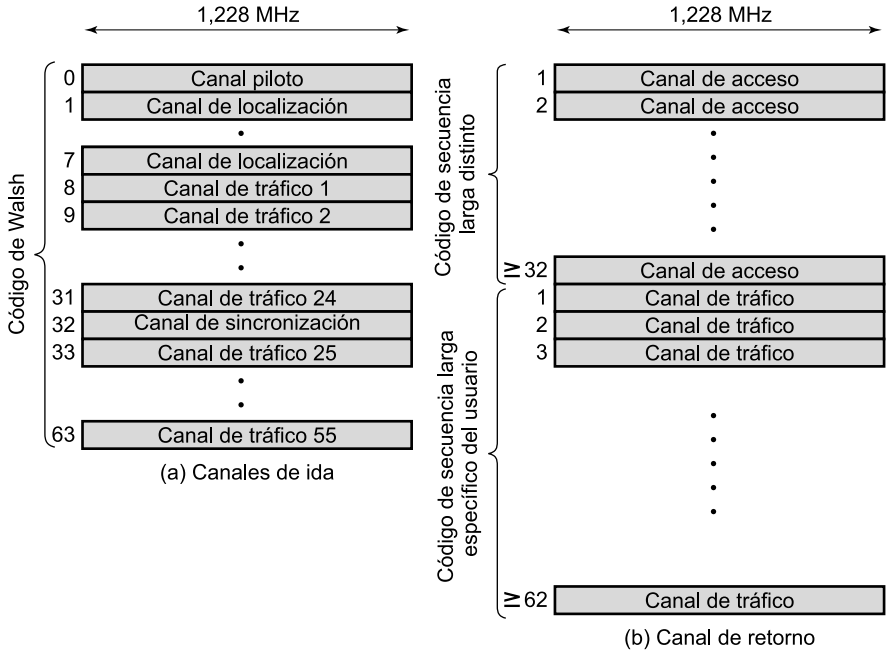


Figura 14.10. Estructura de canales en IS-95.

- **Piloto (canal 0):** transporta una señal continua en un canal único. Este canal permite a la unidad móvil adquirir información de temporización, suministra una fase de referencia para el proceso de demodulación y proporciona un mecanismo para comparar la potencia de la señal con objeto de determinar el traspaso. El canal piloto se compone de una señal con todo ceros.

- **Sincronización (canal 32):** se trata de un canal de 1.200 bps utilizado por la estación móvil para obtener la información de identificación pertinente sobre el sistema celular (tiempo del sistema, estado del código de secuencia larga, revisión del protocolo, etc.).

- **Localización (canales 1 al 7):** contiene mensajes para una o más estaciones móviles.

- **Tráfico (canales 8 al 31 y 33 al 63):** el enlace de ida soporta 55 canales de tráfico. La especificación original soportaba velocidades de transmisión de datos de hasta 9.600 bps. Una revisión posterior añadió un segundo conjunto de velocidades de hasta 14.400 bps.

Obsérvese que todos estos canales utilizan el mismo ancho de banda, utilizándose el código de minibits para distinguir entre ellos. Para el canal de ida, los códigos de minibits son los 64 códigos ortogonales de 64 bits derivados de una matriz 64 × 64 conocida como la matriz de Walsh (analizada en [STAL02]).

La Figura 14.11 muestra las etapas de procesamiento para la transmisión sobre un canal de tráfico de ida usando el conjunto de velocidades 1. Para el tráfico de voz, el habla se codifica a una tasa de datos de 8.550 bps, que resultan en 9.600 bps tras la inserción de bits adicionales para la

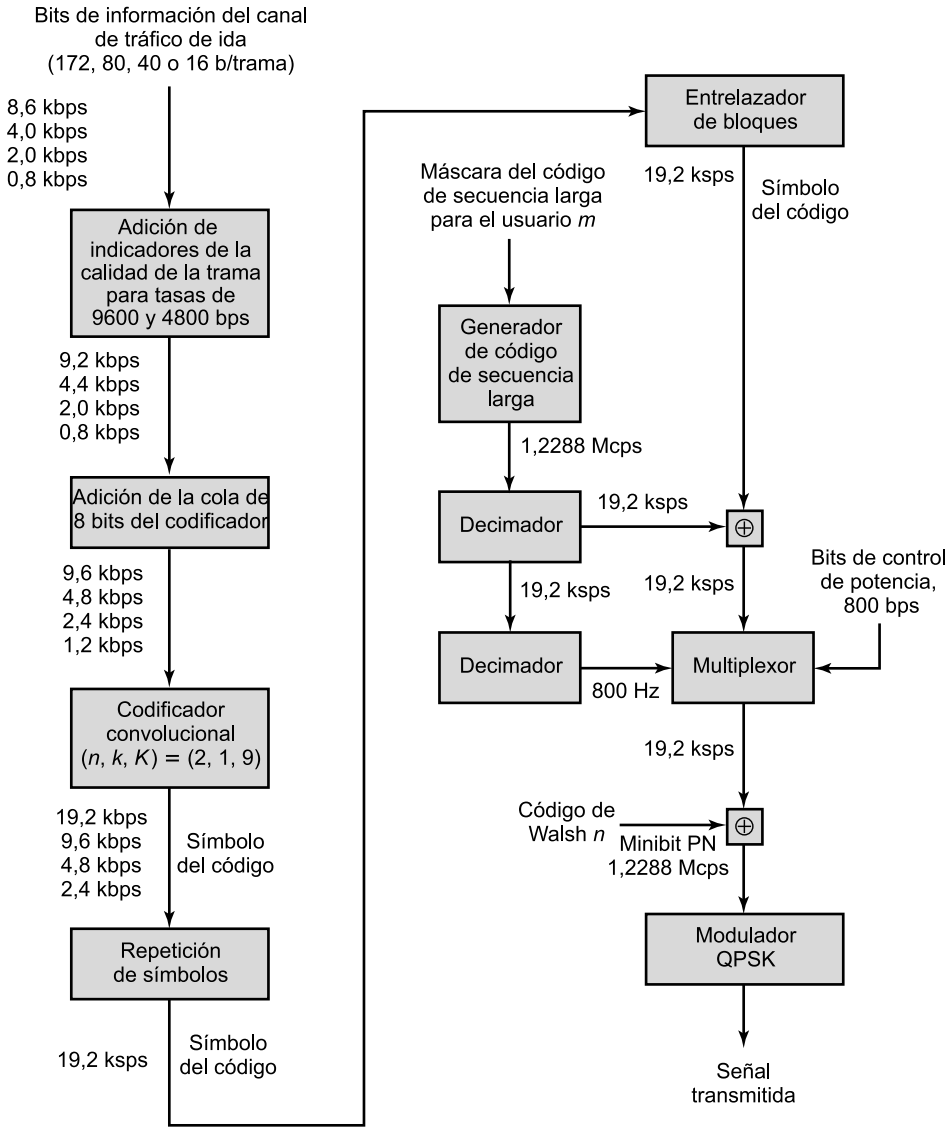


Figura 14.11. Transmisión sobre el enlace de ida en IS-95.

detección de errores. La capacidad total del canal no se emplea cuando el usuario no está hablando. Durante los periodos de silencio, la tasa de datos se reduce incluso hasta 1.200 bps. La tasa de 2.400 bps es utilizada para transmitir transitorios en el ruido de fondo y la de 4.800 bps se usa para combinar el habla digitalizada con datos de señalización.

Los datos o el habla digitalizada se transmiten en bloques de 20 ms con corrección de errores hacia adelante proporcionada por un codificador convolucional con una tasa de 1/2, doblando así la tasa de datos efectiva hasta un máximo de 19,2 kbps. Para tasas de datos inferiores, los bits de salida del codificador (llamados símbolos de código) son replicados hasta alcanzar la tasa de 19,2 kbps. Los datos se entrelazan entonces en bloques para reducir los efectos de los errores mediante su expansión.

A continuación de este entrelazado, los bits de datos son mezclados. El propósito de esta etapa es servir como una máscara de privacidad así como para prevenir el envío de patrones repetitivos, lo que a su vez reduce la probabilidad de que los usuarios transmitan a la potencia de pico al mismo tiempo. La mezcla se lleva a cabo por medio de un código de secuencia larga que se genera como un número pseudoaleatorio a partir de un registro de desplazamiento de 42 bits. El registro de desplazamiento se inicializa con el número electrónico de serie del usuario. La salida del generador del código de secuencia larga se produce a una velocidad de 1,2288 Mbps, que es 64 veces la velocidad de 19,2 kbps, por lo que sólo un bit de cada 64 es seleccionado (por la función de decimación). Al flujo resultante se le aplica la operación XOR con la salida del módulo responsable de entrelazar el bloque.

La siguiente etapa en el procesamiento inserta información concerniente al control de potencia en el canal de tráfico, con objeto de controlar la potencia de salida de la antena. La función de control de potencia de la estación base captura bits del canal de tráfico a una velocidad de 800 bps. Éstos son insertados como bits de código robados. El canal de 800 bps transporta información directamente a la unidad móvil para aumentar, disminuir o mantener estable su nivel de salida actual. Este flujo de control de potencia se multiplexa en los 19,2 kbps reemplazando algunos de los bits de código, usando el generador del código de secuencia larga para codificar los bits.

El siguiente paso en el proceso lo constituye la función DS-SS, que dispersa los 19,2 kbps a una tasa de 1,2288 Mbps utilizando una fila de la matriz 64 × 64 de Walsh. Una fila de la matriz se asigna a una estación móvil durante la configuración de la llamada. Si se presenta un bit 0 a la función XOR, los 64 bits de la fila asignada son enviados. En el caso de un bit 1 se envía el resultado de la función XOR bit a bit de la fila. Así, la tasa de bits final es 1,2288 Mbps. Este flujo digital de bits se modula a continuación sobre la portadora usando un esquema de modulación QPSK. Recuérdese del Capítulo 5 que QPSK incluye la creación de dos flujos de bits que son modulados separadamente (*véase* Figura 5.11). En el sistema IS-95, los datos se dividen en los canales I y Q (en fase y en cuadratura) y a los datos en cada canal se les aplica una operación XOR con un código de secuencia corta único. Los códigos de secuencia corta se generan como números pseudoaleatorios a partir de un registro de desplazamiento de 15 bits.

ENLACE DE RETORNO EN IS-95

En la Tabla 14.4 se listan los parámetros del enlace del canal de retorno. En enlace de retorno se compone de hasta 94 canales lógicos CDMA, cada uno ocupando el mismo ancho de banda de 1228 kHz (*véase* Figura 14.10b). El enlace de retorno soporta hasta 32 canales de acceso y hasta 62 canales de tráfico.

Tabla 14.4. Parámetros de canal para el enlace de retorno en IS-95

Canal	Acceso	Conjunto de velocidades de tráfico 1				Conjunto de velocidades de tráfico 2			
Tasa de datos (bps)	4.800	1.200	2.400	4.800	9.600	1.800	3.600	7.200	14.400
Tasa de código	1/3	1/3	1/3	1/3	1/3	1/2	1/2	1/2	1/2
Tasa de símbolos antes de la repetición (sps)	14.400	3.600	7.200	14.400	28.800	3.600	7.200	14.400	28.800
Repetición de símbolos	2	8	4	2	1	8	4	2	1
Tasa de símbolos tras la repetición (sps)	28.800	28.800	28.800	28.800	28.800	28.800	28.800	28.800	28.800
Ciclo obligatorio de transmisión	1	1/8	1/4	1/2	1	1/8	1/4	1/2	1
Símbolos de código/símbolo de modulación	6	6	6	6	6	6	6	6	6
Minibits PN/símbolo de modulación	256	256	256	256	256	256	256	256	256
Minibits PN/bit	256	128	128	128	128	256/3	256/3	256/3	256/3

Los canales de tráfico en el enlace de retorno son únicos para cada móvil. Cada estación posee una máscara de código de secuencia larga única basada en su número de serie electrónico. La máscara de código largo es un número de 42 bits, lo que permite un total de $2^{42} - 1$ máscaras diferentes. Las unidades móviles usan el canal de acceso para iniciar las llamadas, responder a un mensaje en el canal de localización procedente de la estación base y para actualizaciones de la ubicación.

La Figura 14.12 muestra las etapas de procesamiento para la transmisión sobre el canal de tráfico de retorno utilizando el conjunto de velocidades 1. Las primeras etapas son las mismas que se utilizan en el canal de ida. Para el caso del canal de retorno, el codificador convolucional posee una tasa de 1/3, triplicando así la tasa de datos efectiva hasta un máximo de 28,8 kbps. A continuación, los bloques de datos son entrelazados.

La siguiente etapa consiste en la expansión de los datos usando la matriz de Walsh. Tanto la forma en que se utiliza la matriz como su propósito son diferentes en este caso de los correspondientes al canal de ida. En el canal de retorno, los datos procedentes del entrelazado de bloques están agrupados en unidades de 6 bits. Cada unidad de 6 bits se usa como un índice para seleccionar una fila de la matriz de Walsh 64 × 64 ($2^6 = 64$), de tal forma que la entrada es sustituida por la correspondiente fila. La tasa de datos se ve incrementada así por un factor de 64/6 hasta alcanzar los 307,2 kbps. El objetivo de esta codificación es mejorar la recepción en la estación base. Dado que las 64 codificaciones posibles son ortogonales, la codificación en bloque mejora el algoritmo de toma de decisiones en el receptor y es, además, computacionalmente eficiente (*véase* [PETE95] para más detalles). Es posible ver esta modulación de Walsh como una forma de código de corrección de errores en bloque con $(n, k) = (64, 6)$ y $d_{\min} = 32$. De hecho, todas las distancias son 32.

La introducción de aleatoriedad en la ráfaga de datos se implementa para ayudar a reducir la interferencia con otras estaciones móviles (en [BLAC99b] se expone una discusión). Esta operación incluye el uso de la máscara del código de secuencia larga para suavizar los datos salientes sobre cada trama de 20 ms.

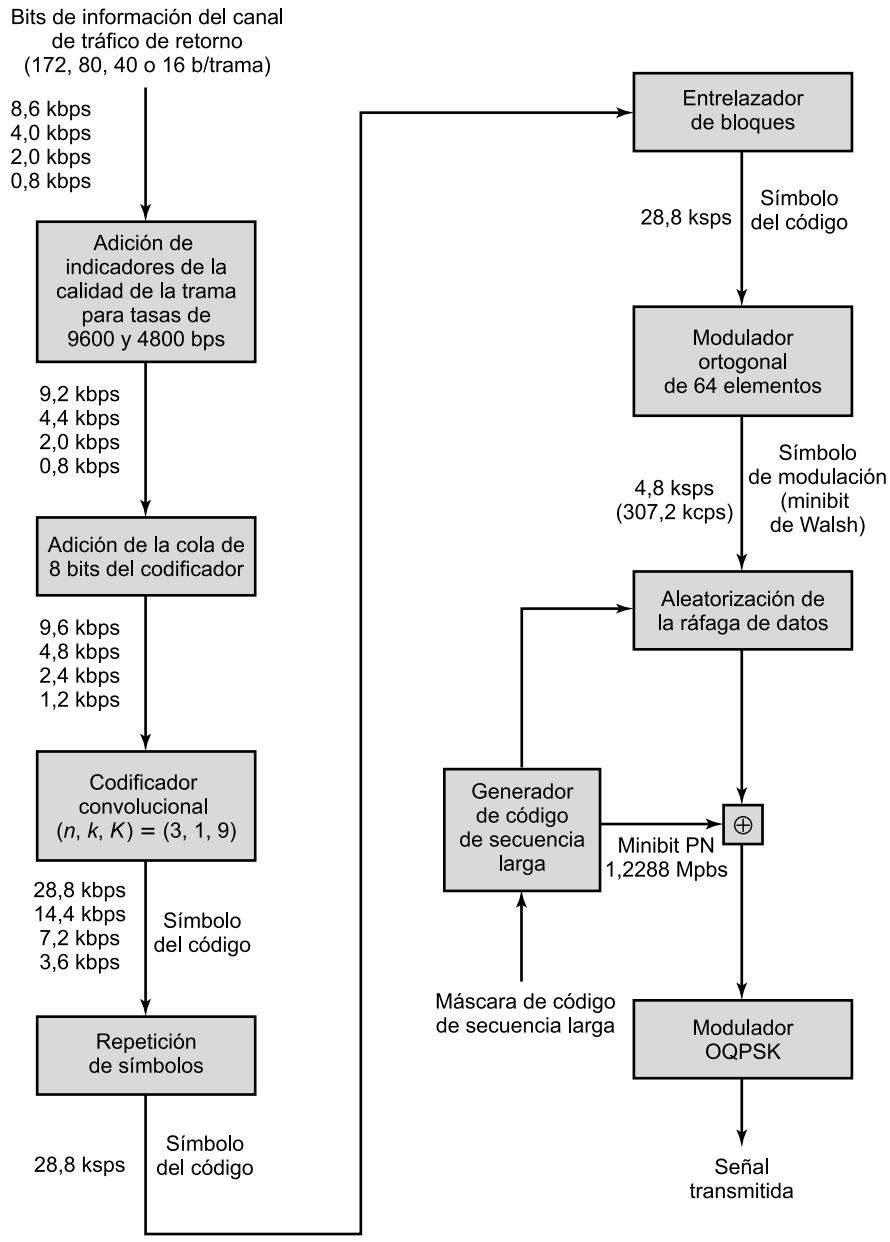


Figura 14.12. Transmisión sobre el enlace de retorno en IS-95.

La siguiente etapa en el proceso está constituida por la función DS-SS. En el caso del canal de retorno, se aplica la operación XOR entre el código de secuencia larga único para el móvil y el flujo de salida tras la aleatorización, produciendo un flujo final de datos de 1,2288 Mbps. Este flujo digital se modula sobre la portadora utilizando un esquema de modulación QPSK ortogonal. Éste se diferencia del utilizado en el canal de ida en el uso de un elemento de retardo en el modulador (*véase* Figura 5.11) con objeto de producir la ortogonalidad. La razón por la que los moduladores son diferentes es que, mientras en el canal de ida los códigos para la dispersión son

ortogonales (procedentes de la matriz de Walsh) en el caso del canal de retorno la ortogonalidad de los códigos de dispersión no está garantizada.

14.4. SISTEMAS DE TERCERA GENERACIÓN

El objetivo de la tercera generación (3G) de comunicaciones inalámbricas es proporcionar adecuadamente comunicaciones inalámbricas de alta velocidad para soportar no sólo voz, sino también multimedia, datos y vídeo. La iniciativa para el año 2000 de las Comunicaciones Móviles Internacionales de la ITU (IMT-2000) ha definido la visión de la ITU de las capacidades de los sistemas de tercera generación como sigue:

- Calidad de voz comparable a la red conmutada pública de telefonía.
- Tasa de datos de 144 kbps disponible para usuarios desplazándose a velocidad elevada en vehículos motorizados sobre una zona extensa.
- 384 kbps disponibles para peatones detenidos o moviéndose a baja velocidad sobre zonas pequeñas.
- Soporte (para ser introducido en una etapa posterior) de 2,048 Mbps para uso de oficina.
- Tasas de transmisión de datos simétricas y asimétricas.
- Soporte para servicios de datos de conmutación de paquetes y conmutación de circuitos.
- Una interfaz adaptativa para Internet que refleje eficientemente la asimetría común entre el tráfico entrante y el saliente.
- Uso más eficiente, en general, del espectro disponible.
- Soporte para una amplia variedad de equipos móviles.
- Flexibilidad para permitir la introducción de nuevos servicios y tecnologías.

En términos generales, una de las directrices que con más fuerza está orientando la tecnología moderna de las comunicaciones es la tendencia hacia servicios de telecomunicaciones personales universales y acceso universal a las comunicaciones. El primero de los términos se refiere a la capacidad de una persona para identificarse fácilmente y usar, como un único abonado, cualquier sistema de comunicaciones en los dominios de un país, un continente, o incluso globalmente. El segundo concepto hace referencia a la capacidad de un usuario para utilizar su terminal en una variedad de entornos para conectarse a los servicios de información (por ejemplo, tener un terminal portátil que funcione igualmente en la oficina, en casa o a bordo de un avión). Esta revolución en la computación personal involucrará, obviamente y de una forma crucial, la presencia de comunicaciones inalámbricas.

Los servicios de comunicaciones personales (PCS, *Personal Communications Services*) y la redes de comunicaciones personales (PCN, *Personal Communications Networks*) son términos inexorablemente relacionados con estos conceptos de comunicaciones inalámbricas globales y forman parte de los objetivos de la tercera generación.

En general, la tecnología que se planifica es digital y utiliza acceso múltiple por división en el tiempo o por división de código para proporcionar una elevada capacidad y un uso eficiente del espectro.

Los terminales de bolsillo para PCS están diseñados para consumir poca potencia y ser relativamente pequeños y ligeros. Se están llevando a cabo esfuerzos considerables internacionalmente para permitir que los mismos terminales puedan ser utilizados en el mundo entero.

INTERFACES ALTERNATIVAS

La Figura 14.13 muestra los esquemas alternativos que han sido adoptados como parte de IMT-2000. La especificación cubre un conjunto de interfaces de radio para optimizar el rendimiento en diferentes entornos de radio. Una de las principales razones para la inclusión de cinco interfaces alternativas era permitir una evolución progresiva a partir de los sistemas existentes de primera y segunda generación y los de 3G.

Las cinco alternativas reflejan la evolución acaecida desde la segunda generación. Dos de las especificaciones surgen del trabajo del Instituto Europeo de Estándares de Telecomunicaciones (ETSI, *European Telecommunications Standards Institute*) para desarrollar un sistema universal de telecomunicaciones móviles (UMTS, *Universal Mobile Telecommunications System*) como estándar inalámbrico europeo de 3G. UMTS incluye dos estándares. Uno de ellos es el conocido como CDMA de banda ancha o W-CDMA. Este esquema explota completamente la tecnología CDMA para proporcionar tasas de datos elevadas con un uso eficiente del ancho de banda. La Tabla 14.5 muestra algunos de los parámetros fundamentales de W-CDMA. El otro esfuerzo europeo bajo UMTS es el conocido como IMT-TC o TD-CDMA. Este enfoque es una combinación de las tecnologías W-CDMA y TDMA. Se pretende que IMT-TC proporcione una infraestructura para la actualización de los sistemas GSM basados en TDMA.

Tabla 14.5. Parámetros de W-CDMA.

Ancho de banda del canal	5 MHz
Estructura del canal RF de ida	Expansión directa
Tasa de minibits	3,84 Mcps
Longitud de trama	10 ms
Número de ranuras/trama	15
Modulación de expansión	QPSK balanceado (ida) Canal dual QPSK (retorno) Circuito de expansión compleja
Modulación de datos	QPSK (ida) BPSK (retorno)
Detección coherente	Símbolos piloto
Multiplexación del canal de retorno	Canales de control y piloto multiplexados en tiempo Multiplexación I y Q para canales de datos y control
Multitasa	Diversas expansiones y multicódigo
Factores de expansión	4 a 256
Control de potencia	Bucle abierto y bucle cerrado rápido (1,6 kHz)
Expansión (ida)	Secuencias ortogonales de longitud variable para la separación de canales. Secuencias estrella (*gold sequences*) 2^{18} para la separación entre usuario y celda.
Expansión (retorno)	Igual que en el de ida, con distintos desplazamientos temporales en los canales I y Q.

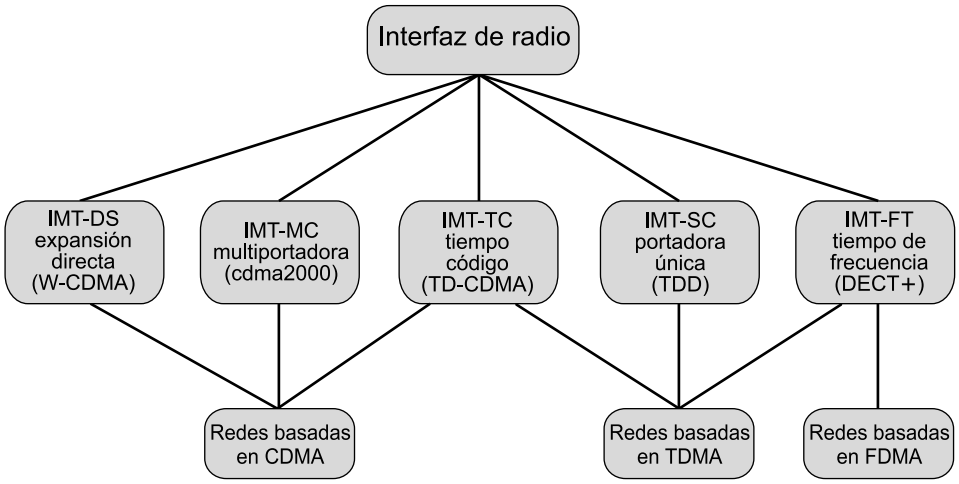


Figura 14.13. Interfaces de radio terrestres de IMT-2000.

Otro sistema basado en CDMA, conocido como cdma2000, tiene un origen norteamericano. Este esquema es similar a W-CDMA, aunque incompatible con él, en parte porque los estándares utilizan diferentes tasas de minibits. Además, cdma2000 utiliza una técnica conocida como multiportadora que no se emplea en W-CDMA.

Las otras dos especificaciones de interfaces se muestran en la Figura 14.13. IMT-SC está diseñado primordialmente para redes que soporten únicamente TDMA. IMT-FC puede ser utilizado tanto por portadoras FDMA como TDMA para proporcionar algunos servicios 3G, procediendo del estándar de telecomunicaciones europeas digitales sin cable (DECT, *Digital European Cordless Telecommunications*).

CONSIDERACIONES DE DISEÑO DE CDMA

La tecnología dominante en los sistemas 3G es CDMA. Aunque se han adoptado tres esquemas CDMA diferentes, todos ellos comparten algunos criterios de diseño. En [OJAN98] se enumeran los siguientes:

- **Ancho de banda:** un objetivo de diseño importante para todos los sistemas 3G es limitar la utilización del canal a 5 MHz. Existen varias razones que justifican este hecho. Por un lado, un ancho de banda de 5 MHz o superior mejora la capacidad del receptor para resolver los efectos multitrayectoria cuando se compara con anchos de banda más reducidos. Por otro lado, el espectro disponible se encuentra limitado por las necesidades de competencia, y 5 MHz es un límite superior razonable que puede ser asignado a los sistemas 3G. Por último, un ancho de banda de 5 MHz es apropiado para soportar tasas de datos de 144 y 384 kbps, siendo éste un objetivo primordial de los servicios 3G.
- **Tasa de minibits:** dado el ancho de banda disponible, la tasa de minibits depende de la tasa de datos deseada, las necesidades de control de errores y las limitaciones del ancho de banda. Una tasa de minibits de 3 Mcps o superior es razonable supuestos estos parámetros de diseño.
- **Multitasa:** el término *multitasa* se refiere a la provisión de múltiples canales lógicos con una tasa de datos fija a un usuario dado, presentando cada canal lógico una tasa diferente.

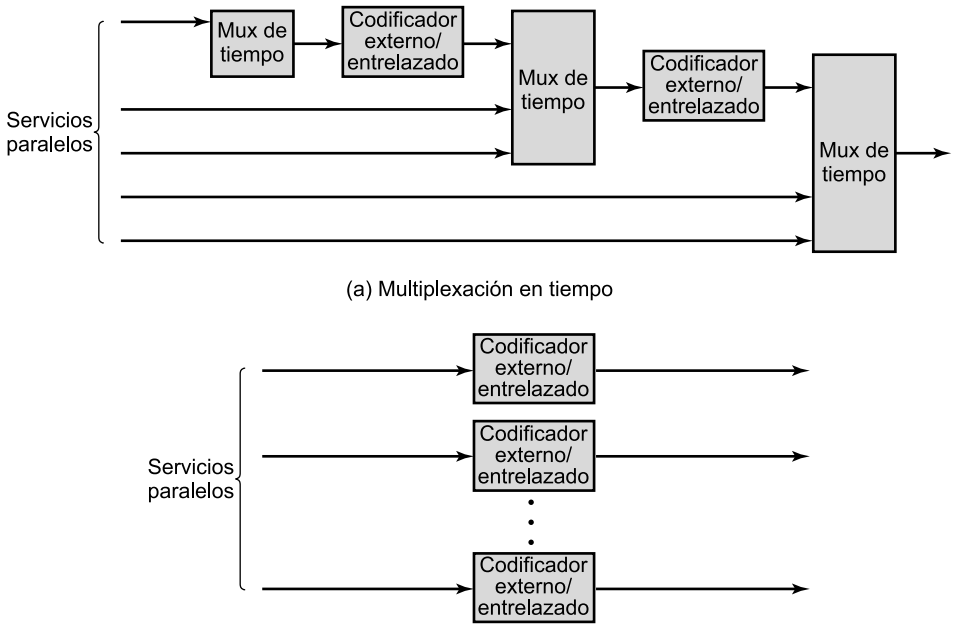


Figura 14.14. Principios de multiplexación en tiempo y por código [OJAN98].

Además, el tráfico en cada canal lógico puede ser conmutado independientemente a través de las redes inalámbricas o fijas hacia diferentes destinos. La ventaja de la multitasa es que el sistema puede soportar de una forma flexible varias aplicaciones simultáneas de un mismo usuario, utilizando de una forma eficiente la capacidad disponible mediante el uso de únicamente aquella capacidad que sea requerida por cada servicio. La multitasa se puede lograr con un esquema TDMA dentro de un mismo canal CDMA, asignando un número diferente de ranuras por trama para conseguir las distintas tasas de datos. Todos los subcanales que operen a una tasa de datos dada podrían ser protegidos mediante técnicas de corrección de errores y entrelazado (*véase* Figura 14.14a). Una alternativa es el uso de varios códigos CDMA, con codificación y entrelazado separados, proyectando cada uno de ellos sobre un canal CDMA diferente (*véase* Figura 14.14b).

14.5. LECTURAS Y SITIOS WEB RECOMENDADOS

[BERT94] y [ANDE95] son revisiones instructivas de los efectos de propagación en comunicaciones celulares inalámbricas. [BLAC99] es uno de los mejores tratamientos técnicos de los sistemas celulares de segunda generación.

[TANT98] contiene reimpresiones de varios artículos importantes concernientes al uso de CDMA en redes celulares. [DINA98] proporciona una introducción de los códigos de expansión, tanto PN como los ortogonales, para redes celulares CDMA.

[OJAN98] proporciona una introducción a las consideraciones técnicas de diseño que son claves para los sistemas 3G. Otra revisión útil es [ZENG00], mientras que [PRAS00] contiene un análisis mucho más detallado.

ANDE95 Anderson, J.; Rappaport, T.; y Yoshida, S. «Propagation Measurements and Models for Wireless Communications Channels.» *IEEE Communications Magazine*, enero 1995.

BERT94 Bertoni, H.; Honcharenko, W.; Maciel, L.; y Xia, H. «UHF Propagation Prediction for Wireless Perrsonal Communications.» *Proceedings of the IEEE*, septiembre 1994.

BLAC99 Black, U. *Second-Generation Mobile and Wireless Networks*. Upper Saddle River, NJ: Prentice Hall, 1999.

DINA98 Dinan, E., y Jabbari, B. «Spreading Codes for Direct Sequence CDMA and Wideband CDMA Cellular Networks.» *IEEE Communications Magazine*, septiembre 1998.

OJAN98 Ojanpera, T., y Prasad, G. «An Overview of Air Interface Multiple Access for IMT-2000/UMTS.» *IEEE Communications Magazine*, septiembre 1998.

PRAS00 Prasad, R.; Mohr, W.; y Konhauser, W., eds. *Third-Generation Mobile Communication Systems*. Boston: Artech House, 2000.

TANT98 Tantaratana, S., y Ahmed, K., eds. *Applications of Spread Spectrum Systems: Selected Readings.* Piscataway, NJ: IEEE Press, 1998.

ZENG00 Zeng, M.; Annamalai, A.; y Bhargava, V. «Harmonization of Global Third-Generation Mobile Systems. *IEEE Communications Magazine*, diciembre 2000.

SITIOS WEB RECOMENDADOS

- **Asociación de Telecomunicaciones Celulares e Internet:** consorcio de industrias que proporciona información sobre diversas aplicaciones de la tecnología inalámbrica.
- **Grupo de Desarrollo CDMA:** contiene, en general, información y enlaces sobre IS-95 y CDMA.
- **3G Americas:** grupo comercial formado por empresas del hemisferio oeste que soportan diversos esquemas de segunda y tercera generación. Contiene noticias de la industria, documentos de formación y otra información técnica.

14.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

Acceso múltiple por división de código (CDMA)
canal de ida
canal de retorno
control de potencia
desvanecimiento
desvanecimiento lento
desvanecimiento plano
desvanecimiento rápido
desvanecimiento selectivo
difracción
dispersión
diversidad
diversidad en frecuencia
diversidad espacial
ecualización adaptativa
estación base
factor de reutilización
radio móvil
red celular

red de primera generación (1G)
red de segunda generación (2G)
red de tercera generación (3G)
reflexión
reutilización de frecuencias
Servicio Avanzado de Telefonía Móvil (AMPS)
traspaso

CUESTIONES DE REPASO

14.1. ¿Qué forma geométrica se utiliza en el diseño de un sistema celular?

14.2. ¿Cuál es el principio de la reutilización de frecuencias en el contexto de una red celular?

14.3. Enumere cinco formas de incrementar la capacidad de un sistema celular.

14.4. Explique la función de localización de un sistema celular.

14.5. ¿Qué es el desvanecimiento?

14.6. ¿Cuál es la diferencia entre la difracción y la dispersión?

14.7. ¿Qué diferencia existe entre el desvanecimiento rápido y el lento?

14.8. ¿Cuál es la diferencia entre el desvanecimiento plano y el selectivo?

14.9. ¿Qué diferencias clave existen entre los sistemas celulares de primera generación y los de segunda generación?

14.10. ¿Qué ventajas presenta el uso de CDMA en una red celular?

14.11. ¿Qué desventajas presenta el uso de CDMA en una red celular?

14.12. ¿Cuáles son algunas de las características fundamentales que distinguen a los sistemas celulares de tercera generación de los de segunda generación?

PROBLEMAS

14.1. Considere cuatro sistemas celulares diferentes que comparten las siguientes características. Las bandas de frecuencia empleadas son de 825 a 845 MHz para la transmisión desde la unidad móvil y de 870 a 890 MHz para la transmisión desde la estación base. Un circuito duplex se compone de un canal de 30 kHz en cada dirección. Los sistemas se distinguen entre sí por el factor de reutilización, que es 4, 7, 12 y 19, respectivamente.

a) Suponga que el grupo de celdas en cada uno de los sistemas (4, 7, 12, 19) se duplica 16 veces. Obtenga el número de comunicaciones simultáneas que pueden ser soportadas por cada uno de los sistemas.

b) Obtenga el número de comunicaciones simultáneas que soporta una celda individual en cada sistema.

c) ¿Cuál es el área cubierta, en número de celdas, por cada sistema?

d) Suponga que el tamaño de celda es el mismo en los cuatro sistemas y que todos ellos cubren una zona fija de 100 celdas. Obtenga el número de comunicaciones simultáneas que pueden ser soportadas por cada sistema.

14.2. Describa una secuencia de eventos similar a la mostrada en la Figura 14.6 para:

a) Una llamada desde una unidad móvil a un abonado fijo.

b) Una llamada desde un abonado fijo a una unidad móvil.

14.3. Un sistema celular analógico posee un ancho de banda asignado de 33 MHz y utiliza dos canales simplex de 25 kHz para proporcionar servicio de voz *full-duplex* y canales de control.

a) ¿Cuál es el número de canales disponibles por celda si se supone un factor de reutilización de frecuencias de (1) 4 celdas, (2) 7 celdas y (3) 12 celdas?

b) Supongamos que se dedica 1 MHz a canales de control, pero solamente se requiere un canal de control por celda. Determínese una distribución razonable de canales de control y de voz por celda para cada uno de los factores de reutilización de frecuencias del punto (a).

14.4. Un sistema celular utiliza FDMA con una asignación de frecuencia de 12,5 MHz en cada dirección, una banda de protección de 10 kHz en el borde de la banda asignada y un ancho de banda de 30 kHz por canal. ¿Cuál es el número de canales disponibles?

14.5. En un sistema celular se define la eficiencia espectral FDMA como $\eta_a = \dfrac{B_c N_T}{B_\omega}$, donde

B_c = ancho de banda de cada canal

B_ω = ancho de banda total en una dirección

N_T = número total de canales de voz en la zona cubierta

¿Cuál es la cota superior de η_a?

PARTE IV

REDES DE ÁREA LOCAL

CUESTIONES DE LA PARTE IV

La tendencia de las redes de área local (LAN) implica el uso de medios de transmisión o conmutación compartidos para lograr altas velocidades de transmisión de datos en distancias relativamente cortas. Varios conceptos clave surgen por sí mismos. Uno es la elección del medio de transmisión. Mientras que el cable coaxial ha sido el medio más usado tradicionalmente, las instalaciones LAN actuales enfatizan el uso de pares trenzados o fibra óptica. En el caso de pares trenzados, se necesitan esquemas de codificación eficientes para lograr velocidades de transmisión altas a través del medio. Las redes LAN inalámbricas están alcanzando también una importancia cada vez mayor. Otro problema de diseño es cómo realizar el control de acceso.

ESQUEMA DE LA PARTE IV

CAPÍTULO 15. VISIÓN GENERAL DE LAS REDES DE ÁREA LOCAL

La tecnología esencial subyacente a todas las formas de LAN incluye: topología, medio de transmisión y técnica de control de acceso al medio. El Capítulo 15 analiza los dos primeros elementos citados. Normalmente se utiliza una de estas cuatro topologías: bus, árbol, anillo o estrella. Los medios de transmisión más comunes para la interconexión en redes locales son el par trenzado (apantallado o no), el cable coaxial (en banda base y banda ancha), la fibra óptica y el medio inalámbrico (microondas e infrarrojo). En este capítulo se describen estas topologías y medios de transmisión, con la excepción del inalámbrico que es tratado en el Capítulo 17.

La creciente difusión de las redes LAN ha conducido a incrementar la necesidad de interconexión de LAN entre ellas y con redes WAN. En el Capítulo 15 también se discute un dispositivo esencial usado para interconectar redes LAN: el puente.

CAPÍTULO 16. REDES LAN DE ALTA VELOCIDAD

El Capítulo 16 examina con detalle las topologías, medios de transmisión y protocolos MAC de los sistemas LAN usuales más importantes; todos ellos han sido definidos en documentos de estandarización. El más importante de ellos es Ethernet, que se ha desarrollado en versiones de 10 Mbps,

100 Mbps, 1 Gbps y 10 Gbps. El capítulo examina a continuación las redes LAN IEEE 802.5 de paso de testigo, concluyendo con una descripción del canal de fibra.

CAPÍTULO 17. REDES LAN INALÁMBRICAS

Las redes LAN inalámbricas utilizan una de las siguientes tres técnicas: espectro expandido, microondas de banda estrecha o infrarrojos. El Capítulo 17 proporciona una visión general de la tecnología y aplicaciones de las redes LAN inalámbricas. El conjunto de estándares más importante concerniente a las redes LAN inalámbricas es el definido por el comité IEEE 802.11. El Capítulo 17 examina también este estándar en profundidad.

CAPÍTULO 15

Visión general de las redes de área local

15.1. Aplicaciones de las redes LAN
Redes LAN de computadores personales
Redes de respaldo y almacenamiento
Redes ofimáticas de alta velocidad
Redes LAN troncales

15.2. Topologías y medios de transmisión
Topologías
Elección de la topología
Elección del medio de transmisión

15.3. Arquitectura de protocolos de redes LAN
Modelo de referencia IEEE 802
Control del enlace lógico
Control de acceso al medio

15.4. Puentes
Funciones de los puentes
Arquitectura de protocolos de los puentes
Encaminamiento estático
Técnica del árbol de expansión

15.5. Conmutadores de la capa 2 y la capa 3
Concentradores
Conmutadores de la capa 2
Conmutadores de la capa 3

15.6. Lecturas y sitios web recomendados

15.7. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

◆ ◆

CUESTIONES BÁSICAS

- Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre los dispositivos y el medio, así como para regular el acceso ordenado al mismo.
- Las topologías usadas para LAN son anillo, bus, árbol y estrella. Una LAN en anillo consiste en un bucle cerrado de repetidores que permite la circulación de los datos alrededor del anillo. Un repetidor puede funcionar también como un punto de conexión de dispositivo, realizándose la transmisión generalmente en forma de tramas. Las topologías en bus y en árbol son secciones pasivas de cable a las que se encuentran conectadas las estaciones, de modo que la transmisión de una trama por parte de una estación puede ser escuchada por cualquier otra estación. Por su parte, una red LAN en estrella incluye un nodo central al que se conectan las estaciones.
- Se ha definido un conjunto de estándares LAN que especifica un rango de velocidades y comprende todas las topologías y medios de transmisión mencionados.
- En la mayoría de los casos, una organización cuenta con varias LAN que precisan estar interconectadas. La solución más sencilla para satisfacer este requisito es el uso de puentes.
- Los centros y los puentes son los componentes básicos de la mayoría de las redes LAN.

◆ ◆

A continuación, se examinan las **redes de área local** (LAN, *Local Area Network*). Mientras que las redes de área amplia o extensa pueden ser tanto públicas como privadas, las LAN son generalmente propiedad de una organización que utiliza la red para interconectar equipos. Las redes LAN tienen mucha mayor capacidad que las de área amplia, permitiendo el transporte de un tráfico interno generalmente superior.

En este capítulo estudiaremos la tecnología subyacente a las redes LAN, así como su arquitectura de protocolos. El Capítulo 16 está dedicado al estudio de sistemas LAN específicos.

15.1. APLICACIONES DE LAS REDES LAN

La variedad de aplicaciones de las redes LAN es amplia. Para comprender el tipo de requisitos que estas redes deben satisfacer, en esta sección se ofrece un breve análisis de algunas de las áreas de aplicación generales más importantes de las redes LAN.

REDES LAN DE COMPUTADORES PERSONALES

Una configuración común de red LAN es aquella que consta de computadores personales. Dado el coste relativamente bajo de estos sistemas, algunos administradores de organizaciones adquieren frecuentemente computadores personales para aplicaciones departamentales, como hojas de cálculo y herramientas de gestión de proyectos, y para el acceso a Internet.

Pero un conjunto de procesadores departamentales no cubre todas las necesidades de un organismo, siendo también necesarios servicios de procesamiento central. Algunos programas, como los modelos de predicción económica, son demasiado grandes para poder ejecutarse en un computador pequeño. Los ficheros de datos corporativos de gran tamaño, como los correspondientes a contabilidad y nóminas, precisan de un servicio centralizado al tiempo que deberían ser accesibles

por parte de distintos usuarios. Además, hay otros tipos de ficheros que, aunque especializados, deben compartirse entre diferentes usuarios. Existen también razones de peso para llevar a cabo la conexión de estaciones de trabajo inteligentes individuales no sólo a un servicio central, sino también entre sí. Los miembros del equipo de un proyecto o de un organismo necesitan compartir trabajo e información, siendo la forma digital la más eficiente para hacerlo.

Algunos recursos caros, como un disco o una impresora láser, pueden ser compartidos por todos los usuarios de una LAN departamental. Además, la red puede servir de nexo entre servicios de red corporativos mayores. Por ejemplo, la compañía puede disponer de una LAN a nivel de edificio y de una red privada de área amplia. Un servidor de comunicaciones puede proporcionar acceso controlado a estos recursos.

El uso de redes LAN para dar soporte a computadores personales y estaciones de trabajo se ha convertido en un hecho casi universal en todo tipo de organizaciones. Incluso en aquellos lugares en los que aún existe una fuerte dependencia con un computador principal se ha transferido parte de la carga de procesamiento a redes de computadores personales. Quizá el mejor ejemplo de la forma en que se utiliza un computador personal sea la implementación de aplicaciones cliente/servidor.

Un requisito importante de las redes de computadores personales es el bajo coste. En particular, el coste de la conexión a la red debe ser significativamente menor que el del dispositivo conectado. Así, para un computador personal típico es deseable que el coste de conexión sea del orden de los cientos de dólares, aceptándose costes de conexión mayores para dispositivos más caros, como estaciones de trabajo de altas prestaciones. En cualquier caso, esto sugiere que la velocidad de la red puede estar limitada, ya que, en general, el coste es superior cuanto mayor sea la velocidad.

REDES DE RESPALDO Y ALMACENAMIENTO

Las redes de respaldo (*backend*) se utilizan para interconectar grandes sistemas como computadores centrales, supercomputadores y dispositivos de almacenamiento masivo. El requisito principal en este caso es la transferencia elevada de datos entre un número limitado de dispositivos en un área reducida, siendo también necesaria generalmente una alta fiabilidad. Entre sus características típicas se encuentran las siguientes:

- **Alta velocidad:** se precisan velocidades de 100 Mbps o más para satisfacer la demanda de alto volumen de tráfico.
- **Interfaz de alta velocidad:** las operaciones de transferencia de datos entre un gran sistema anfitrión y un dispositivo de almacenamiento masivo se realizan generalmente a través de interfaces de entrada/salida en paralelo de alta velocidad, en lugar de a través de interfaces de comunicaciones más lentas. Por tanto, el enlace físico entre la estación y la red debe ser de alta velocidad.
- **Acceso distribuido:** se necesita una técnica de control distribuido de acceso al medio (MAC, *Medium Access Control*) para permitir que varios dispositivos compartan el medio mediante un acceso eficiente y fiable.
- **Distancia limitada:** generalmente las redes de respaldo se emplean en salas de computadores o en un número reducido de habitaciones contiguas.
- **Número limitado de dispositivos:** el número de computadores principales caros y dispositivos de almacenamiento masivo existente en una sala de computadores es generalmente del orden de las decenas.

Generalmente, las redes de respaldo se encuentran en grandes compañías o en instalaciones de investigación con alto presupuesto para procesamiento de datos. Dada la escala referida, una pequeña diferencia en la productividad puede significar millones de dólares.

Consideremos un lugar donde se hace uso de un computador principal dedicado, lo que implica una aplicación grande o un conjunto de aplicaciones. Si la carga crece, el computador principal puede remplazarse por uno más potente, quizá por un sistema multiprocesador. En algunos lugares no basta con colocar un solo sistema, dado que el crecimiento de la demanda supera el aumento de las prestaciones del equipamiento, por lo que se precisarán eventualmente varios computadores independientes. De nuevo, existen razones que fuerzan la interconexión de estos sistemas. El coste de la interrupción del sistema es alto, de modo que debería ser posible, fácil y rápido trasladar las aplicaciones a sistemas de respaldo. Debe ser posible comprobar nuevos procedimientos y aplicaciones sin degradar el sistema de producción. Los ficheros de gran tamaño deben ser accesibles por parte de más de un computador. El balanceado de la carga posibilitaría la maximización de la utilización y de las prestaciones.

Se puede observar que algunos de los requisitos principales para redes de respaldo son diferentes a los de las LAN de computadores personales. Se requieren altas velocidades para poder trabajar adecuadamente, lo que implica generalmente la transferencia de bloques de datos de gran tamaño. Afortunadamente, aunque el coste del equipamiento para conseguir altas velocidades es alto, éste es razonable debido a que el coste de los dispositivos conectados es mucho mayor.

Un concepto relacionado con el de red de respaldo es el de **red de almacenamiento** (SAN, *Storage Area Network*). Una SAN es una red independiente para gestionar las necesidades de almacenamiento. La SAN desliga las tareas de almacenamiento de servidores específicos y crea un servicio de almacenamiento compartido a través de una red de alta velocidad. Entre el conjunto de dispositivos de almacenamiento de la red se pueden encontrar discos duros, unidades de cinta y dispositivos CD. La mayor parte de las SAN hacen uso del canal de fibra descrito en el Capítulo 16. La Figura 15.1 coteja el concepto de red SAN con el concepto tradicional basado en servidores

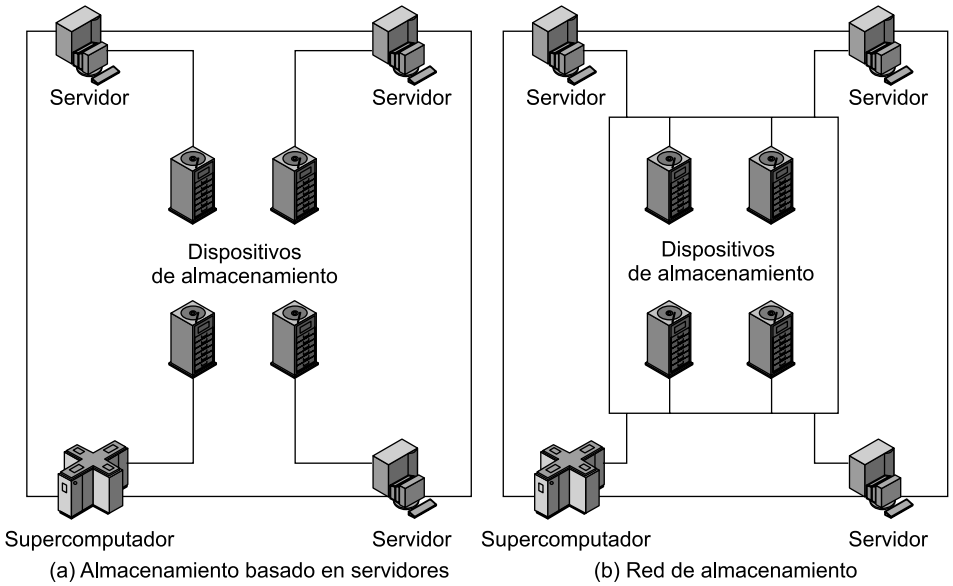


Figura 15.1. Uso de redes de almacenamiento [HURW98].

para el almacenamiento. En una red LAN típica de un tamaño considerable, cada uno de los servidores y supercomputadores posee su propio dispositivo de almacenamiento. Si un cliente necesita acceder a un dispositivo de almacenamiento particular, el acceso debe hacerse a través del servidor que lo controla. En una SAN, por el contrario, no hay servidor alguno entre los dispositivos de almacenamiento y la red, sino que aquellos y los servidores se encuentran directamente conectados a la red. La estructura SAN mejora la eficiencia de acceso de los clientes al almacenamiento, así como las comunicaciones directas de un dispositivo de almacenamiento a otro con la finalidad de realizar copias de respaldo y replicación.

REDES OFIMÁTICAS DE ALTA VELOCIDAD

Tradicionalmente, un entorno ofimático ha incluido una gran variedad de dispositivos con requisitos de transferencia de datos de baja-media velocidad. Sin embargo, las nuevas aplicaciones en el entorno de las oficinas hacen que las limitadas velocidades (hasta 10 Mbps) de las LAN tradicionales resulten inadecuadas. Así, los procesadores de imágenes de sobremesa han incrementado el flujo de datos de red en una cantidad sin precedentes, siendo ejemplos de estas aplicaciones los dispositivos fax, los procesadores de imágenes de documentos y los programas gráficos en computadores personales y estaciones de trabajo. Considérese que una página típica con una resolución de 200 elementos de dibujo, o pel[1] (puntos blancos o negros), por pulgada (resolución adecuada pero no alta) genera 3.740.000 bits (8,5 pulgadas × 11 pulgadas × 40.000 pels por pulgada cuadrada). Incluso haciendo uso de técnicas de compresión, esto generará una carga tremenda. Además, la tecnología y el precio/prestaciones de los discos han evolucionado de forma que son comunes las capacidades de almacenamiento de sobremesa de varios gigabytes. Estas nuevas demandas precisan de redes LAN de alta velocidad que puedan soportar el amplio número y mayor extensión geográfica de los sistemas ofimáticos en comparación con los sistemas existentes en salas de computadores.

REDES LAN TRONCALES

El uso creciente de aplicaciones de procesamiento distribuido y de computadores personales ha provocado la necesidad de una estrategia flexible para el uso de redes LAN. El soporte de las comunicaciones de datos entre oficinas precisa de un servicio de red capaz de cubrir las distancias involucradas y de interconectar equipos situados en un mismo edificio (quizá grande) o en un conjunto de ellos. Aunque es posible desplegar una sola LAN para interconectar todos los equipos de procesamiento de datos de una oficina, no es una alternativa plausible en la mayoría de los casos. Existen varios inconvenientes en una estrategia basada en el uso de una LAN única:

- **Fiabilidad:** una interrupción del servicio, incluso de corta duración, en una LAN única podría provocar un trastorno importante para los usuarios.
- **Capacidad:** una sola LAN se podría saturar cuando el número de dispositivos conectados a la red crezca con el tiempo.
- **Coste:** una tecnología de LAN única no resulta óptima para los numerosos requisitos de interconexión y comunicación. La existencia de un gran número de microcomputadores de

[1] Un *elemento de dibujo*, o *pel*, es la muestra discreta más pequeña de una línea escaneada de un sistema facsímil, que sólo contiene información blanco-negro (no existe escala de grises). Por el contrario, un pixel es un elemento de dibujo que contiene información de escala de grises.

bajo coste obliga a que el soporte de red para estos dispositivos sea también de bajo coste. Las redes LAN que admiten conexiones de muy bajo coste no son adecuadas para satisfacer los requisitos globales.

Una alternativa más atractiva consiste en el empleo de redes LAN de menor coste y capacidad en edificios o departamentos y llevar a cabo la interconexión de estas redes mediante una LAN de mayor capacidad. Esta última red se denomina LAN troncal (*backbone*). Si se encuentra confinada en un solo edificio o conjunto de ellos, una LAN de alta capacidad puede realizar las funciones troncales.

15.2. TOPOLOGÍAS Y MEDIOS DE TRANSMISIÓN

Los principales elementos de una red LAN son los siguientes:

- Topología.
- Medio de transmisión.
- Disposición.
- Técnica de control de acceso al medio.

En su conjunto, estos elementos determinan no sólo el coste y capacidad de la LAN, sino también el tipo de datos que podrán ser transmitidos, la velocidad y eficiencia de las comunicaciones e incluso la clase de aplicaciones que soportará la red.

En esta sección se examinan las principales tecnologías involucradas en los dos primeros puntos anteriormente referidos, viéndose que existe una interdependencia entre la elección que se haga en cada categoría. De acuerdo con esto, resulta más efectivo realizar una discusión sobre los pros y los contras de cada elección examinando ciertas combinaciones preestablecidas. Este enfoque, a su vez, es mejor llevarlo a cabo en el contexto de los estándares que se discutirán en una sección posterior.

TOPOLOGÍAS

En el contexto de una red de comunicaciones, el término *topología* se refiere a la forma según la cual se interconectan entre sí los puntos finales, o estaciones, conectados a la red. Las topologías usuales en redes LAN son bus, árbol, anillo y estrella (*véase* Figura 15.2). El bus es un caso especial de la topología en árbol, con un solo tronco y sin ramas.

Topologías en bus y en árbol

Ambas topologías se caracterizan por el uso de un medio multipunto. En el caso de la topología en **bus**, todas las estaciones se encuentran directamente conectadas, a través de interfaces físicas apropiadas conocidas como tomas de conexión (*taps*), a un medio de transmisión lineal o bus. El funcionamiento *full-duplex* entre la estación y la toma de conexión permite la transmisión y la recepción de datos a través del bus. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de estaciones. En cada extremo del bus existe un terminador que absorbe las señales, eliminándolas del bus.

La topología en **árbol** es una generalización de la topología en bus. El medio de transmisión es un cable ramificado sin bucles cerrados que comienza en un punto conocido como *raíz* o *cabecera*

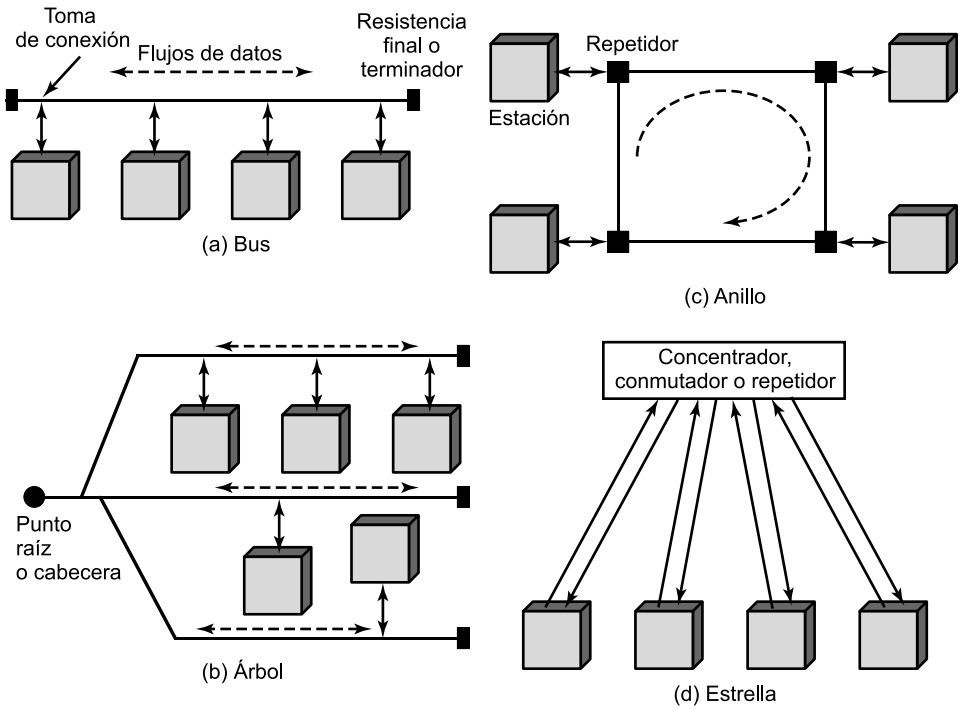


Figura 15.2. Topologías LAN.

(*headend*). Uno o más cables comienzan en el punto raíz y cada uno de ellos puede presentar ramificaciones. Las ramas pueden disponer de ramas adicionales, dando lugar a esquemas más complejos. De nuevo, la transmisión desde una estación se propaga a través del medio y puede alcanzar al resto de estaciones.

Existen dos problemas en esta disposición. En primer lugar, dado que la transmisión desde una estación se puede recibir en las demás estaciones, es necesario algún método para indicar a quién va dirigida la transmisión. En segundo lugar, se precisa un mecanismo para regular la transmisión. Para ver la razón de este hecho hemos de comprender que si dos estaciones intentan transmitir simultáneamente, sus señales se superpondrán y serán erróneas; también se puede considerar la situación en que una estación decide transmitir continuamente durante un largo periodo de tiempo.

Para solucionar estos problemas, las estaciones transmiten datos en bloques pequeños llamados tramas. Cada trama consta de una porción de los datos que una estación desea transmitir además de una cabecera de trama que contiene información de control. A cada estación en el bus se le asigna una dirección, o identificador, única, incluyéndose en la cabecera la dirección destino de la trama.

En la Figura 15.3 se ilustra este esquema. En este ejemplo, la estación C desea transmitir una trama de datos a A, de modo que la cabecera de la trama incluirá la dirección de A. En la propagación de la trama a lo largo del bus, ésta atraviesa B, quien observa la dirección de destino e ignora la trama. A, por su parte, observa que la trama va dirigida a ella y copia los datos de ésta mientras que pasa.

La estructura de la trama resuelve así el primer problema mencionado anteriormente: proporciona un mecanismo para indicar el receptor de los datos. También proporciona una herramienta básica para resolver el segundo problema, el control de acceso. En particular, las estaciones

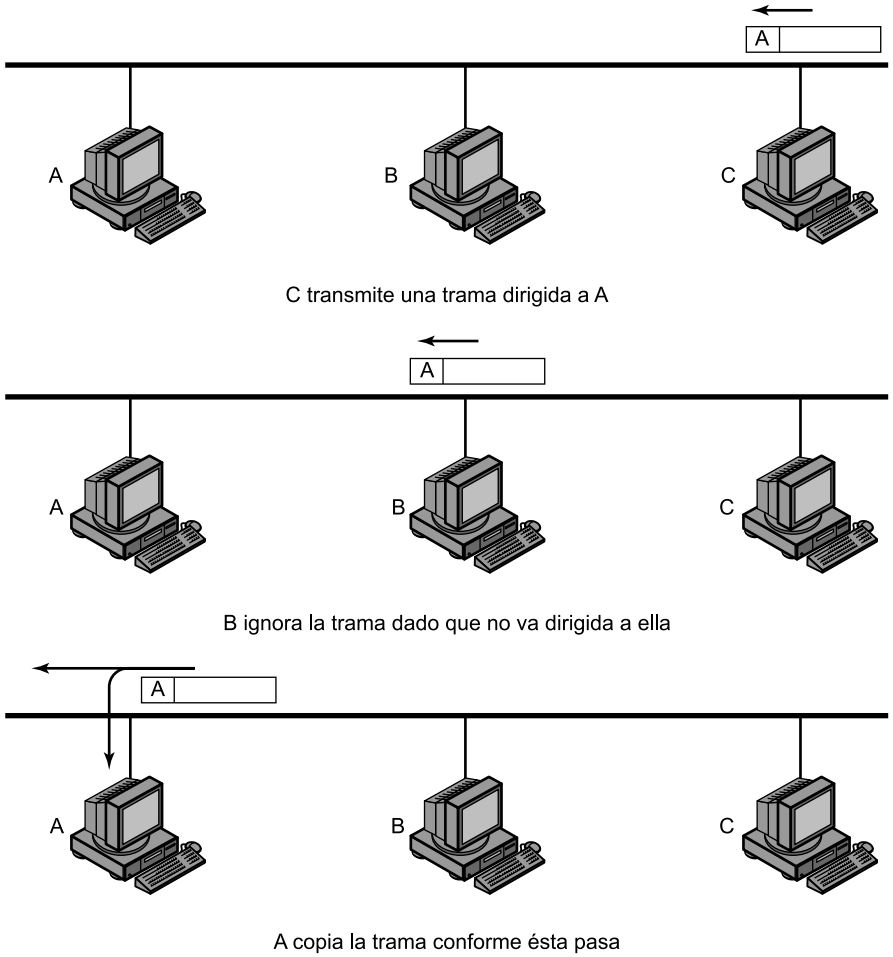


Figura 15.3. Transmisión de tramas en una LAN en bus.

transmiten por turnos de acuerdo con alguna forma cooperativa, lo que implica, como se verá más adelante, el uso de información de control adicional en la cabecera de las tramas.

En la topología en bus o en árbol no son necesarias acciones especiales para eliminar tramas del medio: cuando una señal alcanza el final de éste, es absorbida por el terminador.

Topología en anillo

En la topología en **anillo**, la red consta de un conjunto de *repetidores* unidos por enlaces punto a punto formando un bucle cerrado. El repetidor es un dispositivo relativamente simple, capaz de recibir datos a través del enlace y de transmitirlos, bit a bit, a través del otro enlace tan rápido como son recibidos. Los enlaces son unidireccionales; es decir, los datos se transmiten sólo en un sentido, de modo que éstos circulan alrededor del anillo en el sentido de las agujas del reloj o en el contrario.

Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él. Como en el caso de las topologías en bus y en árbol, los datos se transmiten en

tramas. Una trama que circula por el anillo pasa por las demás estaciones, de modo que la estación de destino reconoce su dirección y copia la trama, mientras ésta la atraviesa, en una memoria temporal local. La trama continúa circulando hasta que alcanza de nuevo la estación origen, donde es eliminada del medio (*véase* Figura 15.4). Dado que el anillo es compartido por varias estaciones, se necesita una técnica de control de acceso al medio para determinar cuándo puede insertar tramas cada estación.

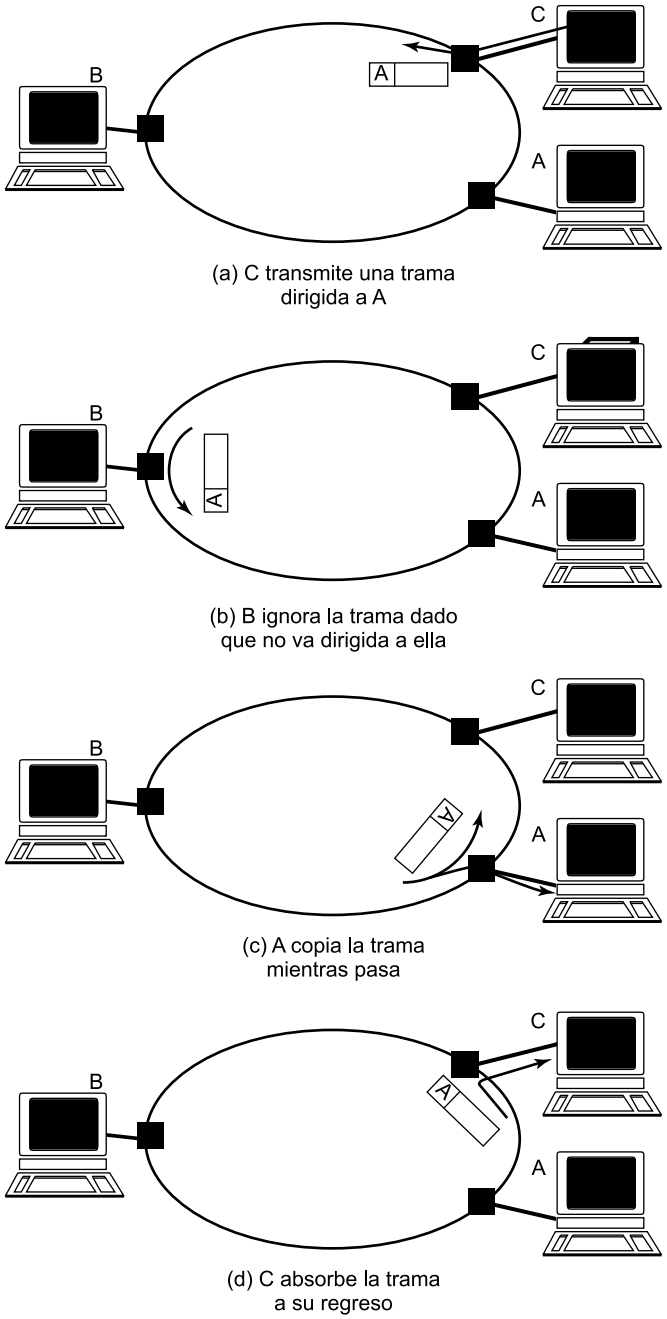


Figura 15.4. Transmisión de tramas en una LAN en anillo.

Topología en estrella

En redes LAN con topología en **estrella** cada estación está directamente conectada a un nodo central común, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción.

En general, existen dos alternativas para el funcionamiento del nodo central. Una es el funcionamiento en modo de difusión, en el que la transmisión de una trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central. En este caso, aunque la disposición física es una estrella, lógicamente funciona como un bus: una transmisión desde cualquier estación es recibida por el resto de estaciones, y sólo puede transmitir una estación en un instante de tiempo dado. En tal caso, al dispositivo central se le conoce como **concentrador** (*hub*). Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena temporalmente en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino. Ambos enfoques son discutidos en la Sección 15.5.

ELECCIÓN DE LA TOPOLOGÍA

La elección de la topología depende de varios factores entre los que se cuentan la fiabilidad de la misma, la capacidad de expansión y el rendimiento. Esta elección forma parte del proceso global de diseño de una LAN y, como tal, no debe ser llevada a cabo independientemente de otros factores, como la elección del medio de transmisión, la disposición del cableado y la técnica de control de acceso. A este respecto se pueden hacer algunas observaciones. Existen cuatro alternativas para el medio de transmisión que pueden ser utilizadas en una LAN en bus:

- **Par trenzado:** en los comienzos del desarrollo de las redes LAN, el par trenzado del tipo utilizado para la transmisión de voz fue usado para proporcionar un bus barato y fácil de instalar, implementándose sobre él varios sistemas a 1 Mbps. Sin embargo, no resulta práctico migrar desde él hacia velocidades más altas en una configuración de bus compartido, por lo que esta alternativa fue descartada hace tiempo.
- **Cable coaxial en banda base:** un cable coaxial en banda base es aquel que hace uso de señalización digital. El esquema original de Ethernet hacía uso de él.
- **Cable coaxial en banda ancha:** se trata del tipo de cable utilizado en los sistemas de televisión por cable. La señalización analógica se utiliza en las frecuencias de radio y televisión. Este tipo de sistema es más caro y más difícil de instalar y mantener que el cable coaxial en banda base. Esta alternativa nunca alcanzó popularidad y las redes basadas en ella ya no se construyen.
- **Fibra óptica:** pese a que la investigación relativa a esta alternativa ha sido considerable en los últimos años, el coste de las tomas de fibra y la disponibilidad de alternativas mejores han ocasionado que esta opción también haya sido descartada.

De esta forma, para el caso de una topología en bus, sólo el cable coaxial en banda base ha alcanzado un uso amplio, principalmente en el caso de los sistemas Ethernet. En comparación con una topología en estrella sobre par trenzado o fibra óptica, resulta más difícil trabajar con una topología en bus con cable coaxial en banda base. Incluso un cambio sencillo puede requerir acceder al cable, mover las tomas y reencaminar los segmentos del mismo. Son pocas las instalaciones nuevas que se realizan siguiendo esta aproximación, aunque, a pesar de todas estas limitaciones, existe una cantidad considerable de redes LAN instaladas sobre este tipo de cable.

La topología en anillo puede ser usada para proporcionar enlaces de muy alta velocidad sobre distancias largas. Un anillo puede proporcionar, potencialmente, mejor rendimiento que cualquier otra topología. Una desventaja, sin embargo, es que un fallo de un solo enlace o de un repetidor puede inutilizar la red entera.

La topología en estrella se aprovecha de la disposición natural del cableado de los edificios. Generalmente, es mejor para distancias cortas y puede ofrecer velocidades elevadas a un número pequeño de dispositivos.

ELECCIÓN DEL MEDIO DE TRANSMISIÓN

La elección del medio de transmisión viene determinada por una serie de factores y se encuentra, como veremos, restringida por la topología de la LAN. Otros aspectos desempeñan un papel importante, entre los que se encuentran los siguientes:

- **Capacidad:** debe soportar el tráfico de red esperado.
- **Fiabilidad:** debe satisfacer los requisitos de disponibilidad.
- **Tipos de datos soportados:** ajustados a la aplicación.
- **Alcance del entorno:** debe proporcionar servicio a la gama de entornos requeridos.

La elección forma parte de la tarea general de diseño de una red local, punto éste que se cubre en el Capítulo 16. Aquí nos limitaremos a realizar algunas observaciones generales.

El par trenzado sin apantallar (UTP) del tipo que se usa para voz es un medio barato y muy bien conocido; se trata del UTP tipo 3 que fue analizado en el Capítulo 4. Generalmente, los edificios de oficinas se encuentran cableados para satisfacer las demandas del sistema telefónico más un margen adicional razonable, por lo que los costes de instalación del cableado son nulos si se usa UTP tipo 3. Sin embargo, la velocidad ofrecida es generalmente bastante limitada, excepto en el caso de redes LAN muy pequeñas. En resumen, el cable UTP tipo 3 es el más idóneo desde el punto de vista del coste para una LAN restringida a un solo edificio y que no soporte demasiado tráfico.

El par trenzado apantallado y el cable coaxial en banda base son más caros que el UTP tipo 3, pero ofrecen una capacidad mayor. El cable coaxial en banda ancha es aún más caro, pero proporciona mayor capacidad. La tendencia de los últimos años ha sido, sin embargo, el uso de UTP de mayor rendimiento, especialmente el de tipo 5. Aunque éste proporciona altas velocidades a un número reducido de dispositivos, es posible construir instalaciones mayores mediante el uso de una topología en estrella. Los conmutadores pueden, más tarde, ser interconectados entre sí mediante diversas configuraciones en estrella. Este punto será analizado en el Capítulo 16.

La fibra óptica resulta atractiva por muchas de sus características, como el aislamiento electromagnético, la alta capacidad y el tamaño reducido, razones éstas por las cuales ha recibido mucha atención. La penetración en el mercado de las redes LAN basadas en fibra óptica es aún reducida. Este hecho se debe principalmente al coste de los componentes de fibra y a la carencia de personal preparado para la instalación y el mantenimiento de los sistemas de fibra. Esta situación está comenzando a cambiar rápidamente a medida que el número de productos basados en fibra está siendo cada vez mayor.

15.3. ARQUITECTURA DE PROTOCOLOS DE REDES LAN

La arquitectura de una LAN se describe mejor en términos de una jerarquía de protocolos que organizan las funciones básicas de la misma. Esta sección comienza con una descripción de la

arquitectura de protocolos estandarizada para redes LAN, que incluye las capas: física, de control de acceso al medio (MAC) y de control de enlace lógico (LLC, *Logical Link Control*). La capa física comprende la topología y el medio de transmisión, y ha sido cubierta en la Sección 15.2. Esta sección ofrece una visión general sobre las capas MAC y LLC.

MODELO DE REFERENCIA IEEE 802

Los protocolos definidos específicamente para la transmisión en redes LAN y MAN tratan cuestiones relacionadas con la transmisión de bloques de datos a través de la red. Según OSI, los protocolos de capas superiores (capa 3 o 4 y superiores) son independientes de la arquitectura de red y son aplicables a redes LAN, MAN y WAN. Así pues, el estudio de protocolos LAN está relacionado con las capas inferiores del modelo OSI.

En la Figura 15.5 se relacionan los protocolos LAN con los de la arquitectura OSI (*véase* Figura 2.6). Esta arquitectura fue desarrollada por el comité IEEE 802 y ha sido adoptada por todas las organizaciones que trabajan en la especificación de los estándares LAN; es la referida como el modelo de referencia IEEE 802.

Desde abajo hacia arriba, la capa inferior del modelo de referencia IEEE 802 es la **capa física** del modelo OSI, e incluye funciones como:

- Codificación/decodificación de señales.
- Generación/eliminación de preámbulo (para sincronización).
- Transmisión/recepción de bits.

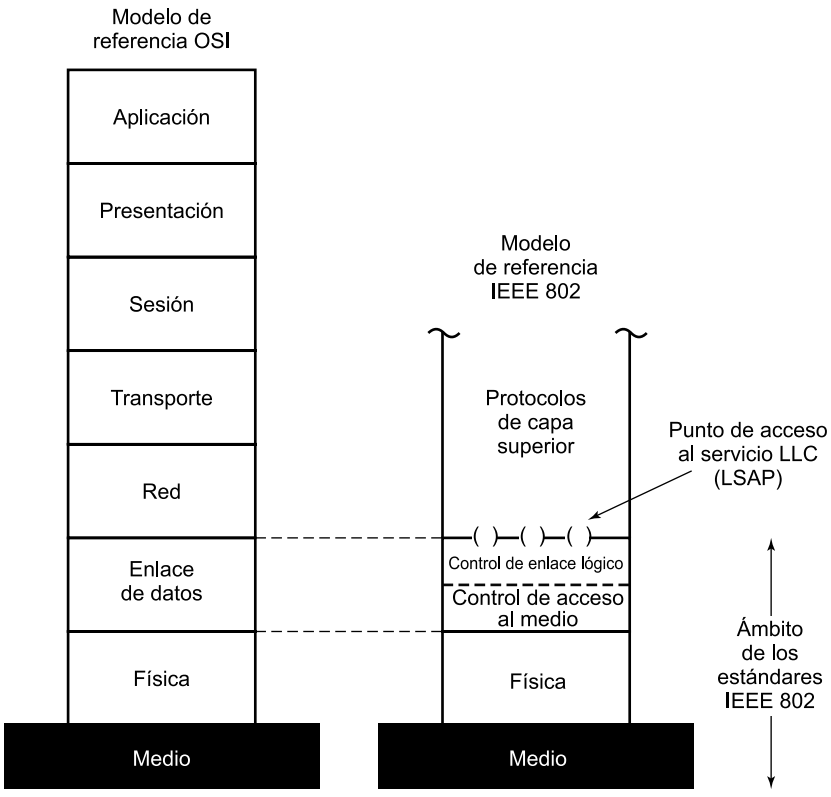


Figura 15.5. Capas del protocolo IEEE 802 en comparación con las del modelo OSI.

Además, la capa física del modelo 802 incluye una especificación del medio de transmisión y de la topología. Generalmente, esto se considera «por debajo» de la capa inferior del modelo OSI. Sin embargo, dado que la elección del medio de transmisión y la topología es crítica en el diseño de redes LAN, se incluye una especificación del medio.

Por encima de la capa física se encuentran las funciones asociadas a los servicios ofrecidos a los usuarios LAN. Entre ellas se encuentran las siguientes:

- En transmisión, ensamblado de datos en tramas con campos de dirección y de detección de errores.
- En recepción, desensamblado de tramas, reconocimiento de dirección y detección de errores.
- Control de acceso al medio de transmisión LAN.
- Interfaz con las capas superiores y control de errores y de flujo.

Estas funciones se asocian generalmente a la capa 2 de OSI. El conjunto de funciones del último punto de los cuatro indicados se agrupan en la capa de **control de enlace lógico (LLC),** mientras que las funciones especificadas en los tres primeros puntos se tratan en una capa separada denominada **control de acceso al medio (MAC).** Esta separación de funciones se debe a las siguientes razones:

- La lógica necesaria para la gestión del acceso a un medio compartido no se encuentra en la capa 2 de control de enlace de datos tradicional.
- Se pueden ofrecer varias opciones MAC para el mismo LLC.

En la Figura 15.6 se ilustra la relación existente entre los niveles de la arquitectura (comparar con la Figura 2.14). Los datos de nivel superior se pasan hacia abajo al nivel LLC, que añade una cabecera de información de control dando lugar a una *unidad de datos de protocolo* (PDU) *LLC*.

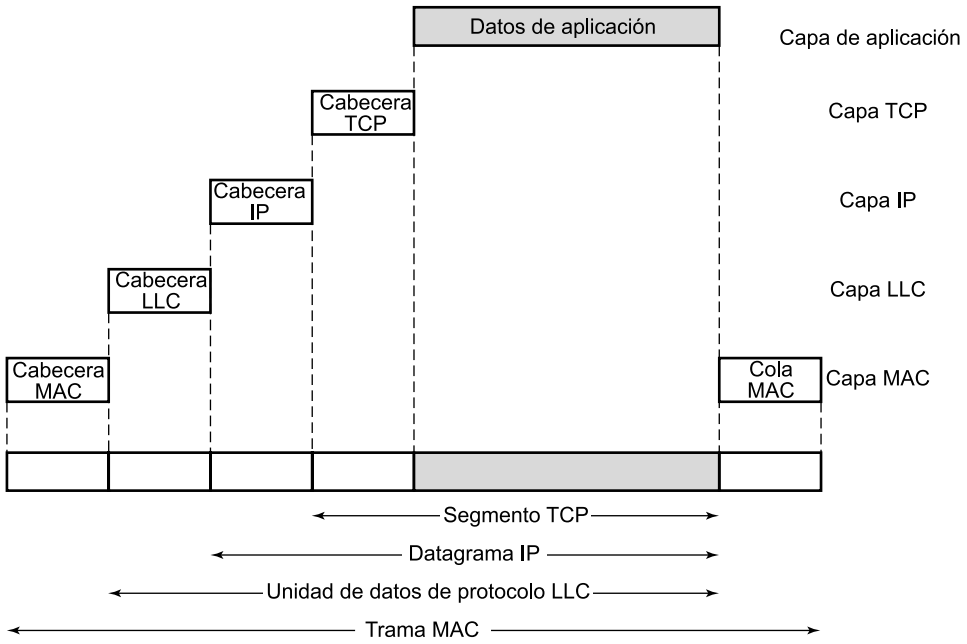


Figura 15.6. Protocolos LAN en contexto.

Esta información de control se utiliza para el funcionamiento del protocolo LLC. La PDU LLC se pasa a la capa MAC, que añade información de control al principio y al final del paquete creando una *trama MAC*. Una vez más, es necesaria la información de control en la trama para el funcionamiento del protocolo MAC. Para situarnos en contexto, la figura muestra también el uso del protocolo TCP/IP y una capa de aplicación por encima de los protocolos LAN.

CONTROL DEL ENLACE LÓGICO

La capa LLC en redes LAN es similar en varios aspectos a otras capas de enlace de uso común. Como todas las capas de enlace, LLC está relacionado con la transmisión de una unidad de datos de protocolo del nivel de enlace (PDU) entre dos estaciones, sin necesitar un nodo de conmutación intermedio. LLC presenta dos características no compartidas por la mayor parte de otros protocolos de control de enlace:

1. Debe admitir el acceso múltiple, consecuencia de la naturaleza de medio compartido del enlace (esto difiere de una línea multipunto en que ahora no existe ningún nodo primario).
2. La capa MAC lo descarga de algunos detalles del acceso al enlace.

El direccionamiento en LLC implica la especificación de los usuarios LLC origen y destino. Normalmente, un usuario es un protocolo de una capa superior o una función de gestión de red en la estación. Manteniendo la terminología OSI para el usuario de una capa de la arquitectura de protocolos, estas direcciones de usuario LLC se denominan puntos de acceso al servicio (SAP, *Service Access Point*).

En primer lugar se estudiarán los servicios que ofrece LLC a un usuario de una capa superior, discutiendo posteriormente el protocolo LLC.

Servicios LLC

LLC especifica los mecanismos para direccionar estaciones a través del medio y para controlar el intercambio de datos entre dos usuarios. El funcionamiento y formato de este estándar están basados en HDLC. Existen tres posibles servicios para dispositivos conectados que usan LLC:

- **Servicio no orientado a conexión sin confirmación:** este servicio es de tipo datagrama. Es muy sencillo, puesto que no incluye mecanismos de control de flujo ni de errores, por lo que no está garantizada la recepción de los datos. En cualquier caso, en la mayoría de los dispositivos existe alguna capa superior de software encargada de gestionar las cuestiones de fiabilidad.
- **Servicio en modo conexión:** este servicio es similar al ofrecido por HDLC. Se establece una conexión lógica entre dos usuarios que intercambian datos, existiendo control de flujo y de errores.
- **Servicio no orientado a conexión con confirmación:** es una mezcla de los dos anteriores. Los datagramas son confirmados, pero no se establece conexión lógica previa.

Generalmente, un vendedor ofrece estos servicios como opciones que el consumidor puede elegir cuando adquiere el equipo. Otra posibilidad es que el consumidor compre un equipo que presente dos o los tres servicios, seleccionando cada uno de ellos de acuerdo con la aplicación.

El **servicio no orientado a conexión sin confirmación** requiere una lógica mínima y es útil en dos situaciones. En primer lugar, en aquellas en las que el software de las capas superiores ofrece

la fiabilidad y los mecanismos de control de flujo necesarios, evitándose la duplicidad. Por ejemplo, TCP podría ofrecer los mecanismos necesarios para asegurar una recepción de datos fiable. En segundo lugar, existen situaciones en las que el coste de establecimiento y mantenimiento de la conexión resulta injustificado e incluso contraproducente (por ejemplo, las actividades de adquisición de datos que implican el muestreo periódico de fuentes de datos, como sensores e informes automáticos de autotest de seguridad de equipos o componentes de red). En una aplicación de supervisión, la pérdida ocasional de datos puede no provocar problemas siempre que el siguiente informe llegue pronto. Así, en la mayoría de los casos, son preferibles los servicios no orientados a conexión sin confirmación.

El **servicio en modo conexión** se puede utilizar en dispositivos muy simples, como controladores de terminal, que disponen de poco software por encima de este nivel. En estos casos, el servicio proporciona mecanismos de control de flujo y de fiabilidad, normalmente implementados en capas superiores del software de comunicaciones.

El **servicio no orientado a conexión confirmado** resulta útil en varias situaciones. Con el servicio en modo conexión, el software de control de enlace lógico debe mantener algún tipo de tabla conteniendo el estado de cada conexión activa. Si el usuario necesita garantizar la recepción, pero existe un gran número de destinos para los datos, el servicio en modo conexión no resulta práctico dado el gran número de tablas necesarias. Un ejemplo es un proceso de control o una empresa automatizada donde es necesario un dispositivo central para comunicar con un gran número de procesadores y controladores programables. Otra posible utilización de este servicio es la gestión de alarmas o señales de control de emergencia de una fábrica: dada su importancia, es necesaria una confirmación, de modo que el emisor pueda estar seguro de que se recibió la señal. Por otro lado, dada la urgencia de la señal, el usuario podría no desear perder tiempo en establecer una conexión lógica como paso previo al envío de los datos.

Protocolo LLC

El protocolo LLC básico se diseñó después de HDLC y presenta funciones y formatos similares a él. Las diferencias entre los dos protocolos se pueden resumir como sigue:

- LLC hace uso del modo de operación balanceado asíncrono de HDLC para dar soporte al servicio LLC en modo conexión. Éste se denomina operación de tipo 2, no empleándose los otros modos de HDLC.
- LLC presta un servicio no orientado a conexión sin confirmación usando la PDU de información no numerada, lo que se conoce como operación de tipo 1.
- LLC ofrece un servicio no orientado a conexión confirmado haciendo uso de dos PDU no numeradas nuevas, lo que se denomina operación de tipo 3.
- LLC permite multiplexación mediante el empleo de puntos de acceso al servicio LLC (LSAP).

Los tres protocolos LLC emplean el mismo formato de PDU (*véase* Figura 15.7), consistente en cuatro campos. Cada uno de los campos DSAP (*Destination Service Access Point*) y SSAP (*Source Service Access Point*) contiene una dirección de 7 bits que especifica los usuarios LLC destino y origen. Un bit del campo DSAP indica si la dirección es individual o de grupo, mientras que un bit de SSAP indica si la PDU es una orden o una respuesta. El formato del campo de control LLC es idéntico al de HDLC (*véase* Figura 7.7), haciendo uso de números de secuencia ampliados (7 bits).

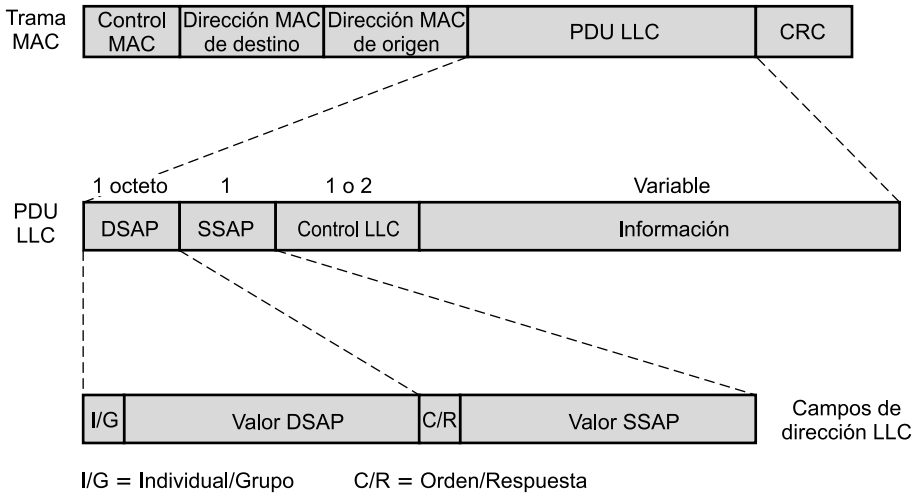


Figura 15.7. PDU LLC con formato genérico de trama MAC.

Para la **operación de tipo 1**, que ofrece el servicio no orientado a conexión no confirmado, se utiliza la PDU de información no numerada (UI, *Unnumbered Information*) para transmitir datos de usuario. No existe confirmación, control de flujo ni control de errores, aunque existe detección de errores y rechazo a nivel MAC.

Otras dos PDU son utilizadas para dar soporte a las funciones de gestión asociadas a los tres tipos de operación. Ambas PDU se usan de la siguiente forma. Una entidad LLC puede emitir una orden (bit C/R = 0) XID o TEST, enviando en respuesta la entidad LLC receptora el correspondiente XID o TEST. La PDU XID se usa para intercambiar dos tipos de información: tipos de operación admitidos y tamaño de ventana. Por su parte, la PDU TEST se emplea para llevar a cabo un test en bucle cerrado del camino de transmisión entre dos entidades LLC. Tras recibir una PDU de orden TEST, la entidad LLC de destino envía, tan pronto como le es posible, una PDU de respuesta TEST.

En la **operación de tipo 2** se establece una conexión de enlace de datos entre dos SAP LLC previamente al intercambio de éstos. El establecimiento de la conexión se intenta por parte del protocolo de tipo 2 en respuesta a una solicitud de un usuario. La entidad LLC envía una PDU SABME[2] para solicitar una conexión lógica con la otra entidad LLC. Si el usuario LLC especificado en el campo DSAP acepta la conexión, la entidad de destino LLC devuelve una PDU de confirmación no numerada (UA, *Unnumbered Acknowledgment*). La conexión queda identificada unívocamente por el par de SAP de usuario. Si el usuario LLC destino rechaza la solicitud de conexión, su entidad LLC devuelve una PDU de modo desconectado (DM, *Disconnected Mode*).

Una vez que la conexión está establecida, los datos se intercambian, como en HDLC, haciendo uso de PDU de información. Las PDU de información contienen los números de secuencia enviado y recibido para la gestión del orden secuencial y el control de flujo. Como en HDLC, las PDU de supervisión se utilizan para el control de errores y de flujo. Cualquiera de las dos entidades LLC puede terminar una conexión LLC lógica mediante el envío de una PDU de desconexión (DISC).

[2] SABME significa Establecer el Modo Balanceado Ampliado Asíncrono (*Set Asynchronous Balanced Mode Extended*). Se usa en HDLC para elegir ABM y seleccionar números de secuencia ampliados de 7 bits. Tanto ABM como los números de secuencia de 7 bits son obligatorios en la operación de tipo 2.

En la **operación de tipo 3** se confirma cada PDU transmitida. Se define una nueva PDU no numerada (no existente en HDLC): la de información no orientada a conexión con confirmación (AC, *Acknowledged Connectionless*). Los datos de usuario se envían en sucesivas PDU de orden AC, y deben ser confirmadas usando una PDU de respuesta AC. Para prevenir las pérdidas de PDU se utiliza un número de secuencia de 1 bit, de forma que el emisor alterna el uso de 0 y 1 en sus PDU de orden AC y el receptor responde con una PDU AC con el número opuesto al de la orden correspondiente. Sólo se puede enviar una PDU en cada sentido en un instante de tiempo dado.

CONTROL DE ACCESO AL MEDIO

Todas las LAN y MAN constan de un conjunto de dispositivos que deben compartir la capacidad de transmisión de la red, de manera que se requiere algún método de control de acceso al medio con objeto de hacer un uso eficiente de esta capacidad. Ésta es la función del protocolo de control de acceso al medio (MAC).

Los parámetros clave en cualquier técnica de control de acceso al medio son dónde y cómo. *Dónde* se refiere a si el control se realiza de forma centralizada o distribuida. En un esquema centralizado se diseña un controlador con autoridad para conceder el acceso a la red, de modo que una estación que desee transmitir debe esperar hasta que se le conceda permiso por parte del controlador. En una red descentralizada, las estaciones realizan conjuntamente la función de control de acceso al medio para determinar dinámicamente el orden en que transmitirán. Un esquema centralizado presenta ciertas ventajas, entre las que se encuentran:

- Puede mejorar el control de acceso proporcionando prioridades, rechazos y capacidad garantizada.
- Permite el uso de una lógica de acceso relativamente sencilla en cada estación.
- Resuelve problemas de coordinación distribuida entre entidades paritarias.

Las principales desventajas de los esquemas centralizados son:

- Genera un punto de falla; es decir, existe un punto en la red tal que si se produce un fallo en él, fallará toda la red.
- Puede actuar como un cuello de botella, reduciendo las prestaciones.

Los pros y contras de los esquemas distribuidos son los contrarios de los puntos anteriores.

El segundo parámetro, *cómo*, viene impuesto por la topología y es un compromiso entre factores como el coste, las prestaciones y la complejidad. En general, podemos clasificar las técnicas de control de acceso como síncronas o asíncronas. Con las técnicas síncronas se dedica una capacidad dada a una conexión. Ésta es la misma aproximación usada en conmutación de circuitos, multiplexación por división en frecuencias (FDM) y multiplexación por división en el tiempo síncrona (TDM). Estas técnicas no son óptimas en redes LAN y MAN dado que las necesidades de las estaciones son impredecibles. Es preferible, por tanto, tener la posibilidad de reservar capacidad de forma asíncrona (dinámica) más o menos en respuesta a solicitudes inmediatas. La aproximación asíncrona se puede subdividir en tres categorías: rotación circular, reserva y contención.

Rotación circular

Con la técnica de rotación circular se le da a cada estación la oportunidad de transmitir, ante lo que la estación puede declinar la proposición o puede transmitir sujeta a un límite superior, especificado

generalmente en términos de cantidad de datos a transmitir o tiempo para ello. En cualquier caso, cuando la estación termina debe ceder el turno de transmisión a la siguiente estación en la secuencia lógica. El control de secuencia puede ser centralizado o distribuido, siendo el método de sondeo un ejemplo de técnica centralizada.

Cuando varias estaciones disponen de datos a transmitir durante un largo periodo de tiempo, las técnicas de rotación circular pueden resultar muy eficientes. En cambio, si sólo unas pocas estaciones disponen de datos a transmitir durante un extenso periodo de tiempo existirá un coste considerable en el paso del turno entre estaciones, ya que la mayoría de ellas no transmiten datos sino que solamente ceden el turno. En estas circunstancias pueden ser preferibles otras técnicas dependientes de si el tráfico de datos es a ráfagas o continuo. El tráfico continuo se caracteriza por transmisiones largas y razonablemente continuas; algunos ejemplos son la comunicación de voz, la telemetría y la transferencia de ficheros grandes. Por su parte, el tráfico a ráfagas se caracteriza por transmisiones cortas y esporádicas, como en el caso de tráfico interactivo terminal-estación.

Reserva

Las técnicas de reserva son adecuadas para tráfico continuo. Generalmente, en estas técnicas se divide el tiempo en ranuras, como en el caso de la técnica TDM síncrona. Una estación que desea transmitir reserva futuras ranuras para un largo, incluso indefinido, periodo de tiempo. Una vez más, las reservas se pueden llevar a cabo de forma centralizada o distribuida.

Contención

Por lo general, las técnicas de contención son apropiadas para tráfico a ráfagas. Con estas técnicas no se realiza control para determinar de quién es el turno, sino que todas las estaciones compiten en una forma que puede ser, como veremos, bastante ruda y caótica. Estas técnicas son necesariamente de naturaleza distribuida, radicando su principal ventaja en el hecho de que son sencillas de implementar y eficientes en condiciones de carga baja o moderada. Sin embargo, para algunas de estas técnicas las prestaciones tienden a deteriorarse bajo condiciones de alta carga.

Aunque tanto las técnicas de reserva centralizadas como las distribuidas se implementan en algunos productos LAN, las más comunes son las técnicas de rotación circular y de contención.

Formato de trama MAC

La capa MAC recibe un bloque de datos de la capa LLC y debe realizar funciones relacionadas con el acceso al medio y la transmisión de datos. Como en otras capas de la arquitectura de protocolos, MAC implementa estas funciones haciendo uso de una unidad de datos de protocolo (PDU) a la que se denomina trama MAC.

El formato exacto de la trama MAC difiere ligeramente para los distintos protocolos MAC en uso. En general, todas las tramas MAC tienen un formato similar al de la Figura 15.7. Los campos de esta trama son:

- **Control MAC:** este campo contiene información de control de protocolo necesaria para el funcionamiento del protocolo MAC. Por ejemplo, aquí se podría indicar un nivel de prioridad.
- **Dirección MAC de destino:** punto de conexión física MAC en la LAN del destino de la trama.

- **Dirección MAC de origen:** punto de conexión física MAC en la LAN del origen de la trama.
- **LLC:** datos LLC de la capa inmediatamente superior.
- **CRC:** campo de comprobación de redundancia cíclica, también conocido como campo de secuencia de comprobación de trama (FCS, *Frame Check Sequence*). Como se vio en HDLC y en otros protocolos de control de enlace de datos (*véase* Capítulo 7), este campo es un código de detección de errores.

En la mayor parte de los protocolos de control del enlace de datos, la entidad del protocolo de nivel de enlace es responsable, no sólo de la detección de errores haciendo uso del campo CRC, sino también de la recuperación de éstos mediante la retransmisión de las tramas erróneas. En la arquitectura de protocolos LAN, estas dos funciones se dividen entre las capas MAC y LLC. La capa MAC es responsable de la detección de errores y del rechazo de tramas erróneas. Opcionalmente, la capa LLC controla qué tramas han sido recibidas correctamente y retransmite las erróneas.

15.4. PUENTES

Casi siempre existe la necesidad de llevar a cabo la expansión más allá de los límites de una LAN para proporcionar interconexión con otras LAN y con redes de área amplia. Dos aproximaciones generales se utilizan con este fin: puentes y dispositivos de encaminamiento. El uso de puentes es la aproximación más sencilla y permite la interconexión de LAN similares, mientras que los dispositivos de encaminamiento son de propósito más general y posibilitan la interconexión de una gran variedad de redes LAN y WAN. En esta sección se lleva a cabo el estudio de los puentes, dejándose el de los dispositivos de encaminamiento para la Parte V del libro.

Los puentes se han diseñado para su uso entre redes de área local (LAN) que utilizan protocolos idénticos en las capas física y de acceso al medio (por ejemplo, todas siguiendo la norma IEEE 802.3). Dado que todos los dispositivos usan los mismos protocolos, el volumen de procesamiento necesario en el puente es mínimo. Los puentes más sofisticados permiten la conversión entre formatos MAC diferentes (por ejemplo, la interconexión de una LAN Ethernet con una en anillo con paso de testigo).

Dado que los puentes se utilizan en situaciones en las que todas las LAN tienen las mismas características, el lector puede preguntarse por qué no utilizar simplemente una LAN mayor. Dependiendo de ciertas circunstancias, existen varias razones para el empleo de varias LAN interconectadas mediante puentes:

- **Fiabilidad:** el peligro en la conexión de todos los dispositivos de procesamiento de datos de un organismo en una sola red es que un fallo en ella puede imposibilitar la comunicación para todos los dispositivos. En cambio, haciendo uso de puentes, la red puede dividirse en unidades autocontenidas.
- **Prestaciones:** en general, las prestaciones de una LAN decrecen cuando aumenta el número de dispositivos o la longitud del medio. A veces, varias LAN pequeñas pueden ofrecer mejores prestaciones si se pueden agrupar los dispositivos de manera tal que el tráfico interno de cada red supere significativamente el tráfico entre ellas.
- **Seguridad:** la disposición de varias LAN puede mejorar la seguridad en las comunicaciones. Es deseable mantener diferentes tipos de tráfico (por ejemplo, contabilidad, personal, planificación estratégica) con necesidades diferentes de seguridad y en medios separados

físicamente. Simultáneamente a este hecho, los diferentes tipos de usuarios con diferentes niveles de seguridad necesitan comunicarse mediante mecanismos controlados y supervisados.

- **Geografía:** es evidente que se necesitan dos LAN separadas para dar soporte a dispositivos agrupados en dos lugares geográficamente distantes. Incluso en el caso de dos edificios separados por una carretera, resulta más fácil usar como puente un enlace de microondas que intentar disponer un cable coaxial entre los dos edificios.

FUNCIONES DE LOS PUENTES

En la Figura 15.8 se ilustra el funcionamiento de un puente que conecta dos redes LAN, A y B, que utilizan el mismo protocolo MAC. En este ejemplo, el puente se conecta a ambas redes, si bien, usualmente, la función de puente se lleva a cabo mediante dos «semipuentes», uno conectado a cada LAN. Las funciones del puente son pocas y sencillas:

- Lectura de todas las tramas transmitidas en A y aceptación de aquellas dirigidas a estaciones en B.
- Retransmisión hacia B de cada una de las tramas, haciendo uso del protocolo de control de acceso al medio de esta LAN.
- El mismo proceso para el tráfico de B a A.

Merece la pena resaltar varios aspectos del diseño de los puentes:

- El puente no modifica el contenido o formato de las tramas que recibe ni las encapsula con una cabecera adicional. Cada trama a transmitir es simplemente copiada desde una LAN y repetida con, exactamente, el mismo patrón de bits en la otra LAN. Esto se puede hacer así dado que las dos LAN usan los mismos protocolos.

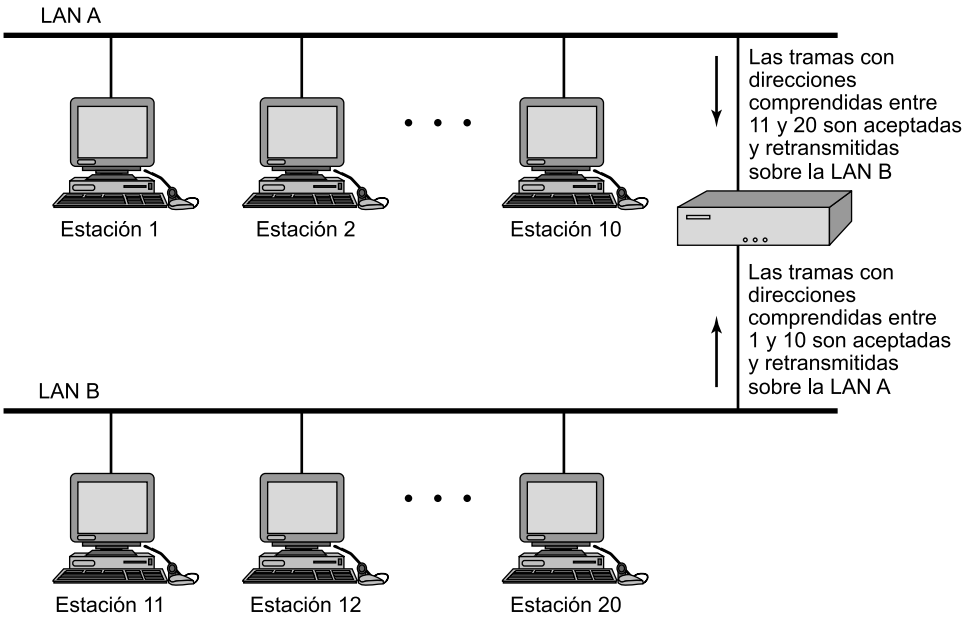

LAN A
Las tramas con direcciones comprendidas entre 11 y 20 son aceptadas y retransmitidas sobre la LAN B
Estación 1
Estación 2
Estación 10
Las tramas con direcciones comprendidas entre 1 y 10 son aceptadas y retransmitidas sobre la LAN A
LAN B
Estación 11
Estación 12
Estación 20

Figura 15.8. Funcionamiento de los puentes.

- El puente debe disponer de suficiente memoria temporal para aceptar demandas de pico. Para un periodo de tiempo pequeño, las tramas se pueden recibir más rápidamente de lo que se pueden retransmitir.
- El puente debe presentar capacidad de direccionamiento y de encaminamiento. Como mínimo, debe conocer las direcciones de cada red para determinar qué tramas debe pasar. Además, pueden existir más de dos redes LAN interconectadas por varios puentes, en cuyo caso puede ser necesario encaminar una trama a través de varios puentes a lo largo de su trayecto desde el origen hasta el destino.
- Un puente puede conectar más de dos LAN.

En resumen, el puente permite una ampliación de las LAN de tal manera que no se precisa modificar el software de comunicaciones de las estaciones conectadas a ellas. Desde el punto de vista de cada una de las estaciones en las dos (o más) LAN, parece como si sólo existiese una única red LAN en la que cada estación tiene una dirección única. Las estaciones utilizan esa dirección única y no necesitan discriminar explícitamente entre estaciones en la misma o en diferentes LAN; el puente se encarga de ello.

ARQUITECTURA DE PROTOCOLOS DE LOS PUENTES

La especificación IEEE 802.1D define la arquitectura de protocolos para puentes MAC. En la arquitectura 802, la dirección final o de estación se establece en el nivel MAC, de modo que es a este nivel al que puede funcionar un puente. En la Figura 15.9 se muestra el caso más simple, consistente en dos LAN con los mismos protocolos MAC y LLC conectadas por un único puente. El puente funciona como se ha descrito anteriormente: captura las tramas MAC cuyo destino no se encuentra en la LAN de origen, las almacena temporalmente y las transmite sobre la otra LAN. Por lo que se refiere a la capa LLC, existe un diálogo entre las entidades LLC paritarias en las dos estaciones finales, no conteniendo el puente esta capa dado que su única función es la retransmisión de las tramas MAC.

En la Figura 15.9b se indica la forma en que se encapsulan los datos en un puente. Éstos se ofrecen al protocolo LLC por parte de algún usuario. La entidad LLC añade una cabecera y pasa la unidad de datos resultante a la entidad MAC, que añade una cabecera y una cola para dar lugar a una trama MAC. El puente captura la trama de acuerdo con la dirección MAC de destino especifi-

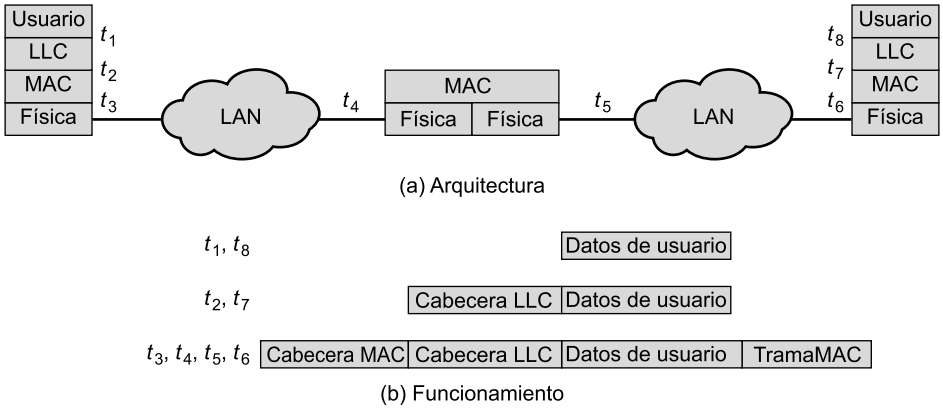


Figura 15.9. Conexión de dos redes LAN mediante un puente.

cada en ella y, dado que su función es retransmitirla intacta a la LAN destino, no elimina los campos MAC. De esta forma, la trama se deposita en la LAN destino y es capturada por la estación destino.

El concepto de puente de retransmisión MAC no está limitado al uso de un único puente para conectar dos LAN adyacentes. Si las LAN están distanciadas, se pueden conectar a través de dos puentes intercomunicados. La comunicación entre los dos puentes puede consistir en una red, de conmutación de paquetes de área amplia por ejemplo, o en un enlace punto a punto. En estos casos, cuando un puente captura una trama MAC, debe encapsularla apropiadamente y transmitirla sobre la conexión hacia el otro puente, el cual eliminará los campos extra y transmitirá la trama MAC en su forma original a la estación de destino.

ENCAMINAMIENTO ESTÁTICO

Existe una tendencia en muchas organizaciones hacia un aumento del número de redes LAN interconectadas mediante puentes. Cuanto mayor es este número, más importante resulta proporcionar rutas alternativas entre LAN a través de puentes para cuestiones de balanceado de carga y reconfiguración en caso de aparición de fallos. De este modo, muchas organizaciones encuentran que las tablas de encaminamiento estáticas predefinidas resultan inadecuadas, siendo necesario algún tipo de encaminamiento dinámico.

Considérese la configuración dada en la Figura 15.10. Supongamos que la estación 1 transmite una trama sobre la LAN A con destino a la estación 6. La trama se recibirá en los puentes 101, 102

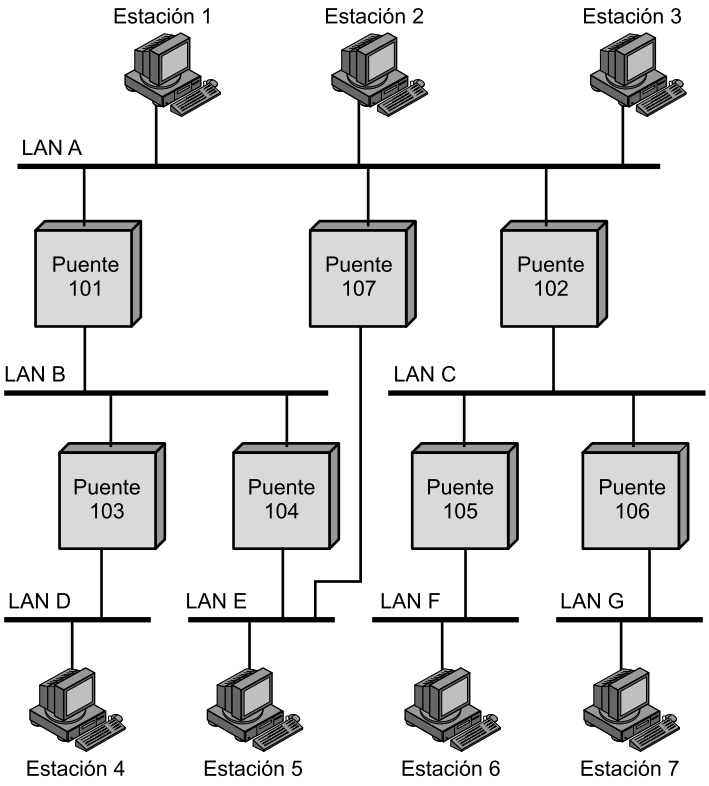


Figura 15.10. Configuración de puentes y redes LAN con rutas alternativas.

y 107, de forma que todos ellos determinarán que la estación de destino no se encuentra en una de las LAN a las que están conectados. Por tanto, cada puente tomará una decisión acerca de si retransmitir o no la trama sobre sus otras LAN con objeto de dirigirla hacia el destino deseado. En este caso, el puente 102 debería repetir la trama sobre la LAN C, mientras que los puentes 101 y 107 decidirán no llevar a cabo la retransmisión de la trama. Una vez que la trama se ha enviado sobre la LAN C, se recibirá en los puentes 105 y 106, los cuales, como antes, deben decidir si retransmitirla o no. En caso de su retransmisión, el puente 105 puede hacerlo sobre la LAN F, donde la trama será finalmente recibida por la estación de destino 6.

Se observa que, en el caso general, el puente debe disponer de capacidad de encaminamiento, de modo que cuando un puente recibe una trama debe decidir si llevar a cabo o no su retransmisión. Si el puente se encuentra conectado a dos o más redes, debe decidir si retransmitir la trama o no y, en su caso, sobre qué LAN hacerlo.

La decisión de encaminamiento puede no resultar siempre tan sencilla. En la Figura 15.10 se muestra la existencia de dos rutas entre las LAN A y E. Esta redundancia proporciona una disponibilidad superior en la interconexión de las redes, posibilitando el balanceado de la carga. En este caso, si la estación 1 transmite una trama a través de la LAN A dirigida a la estación 5 de la LAN E, los puentes 101 o 107 pueden retransmitir la trama. Parece más adecuado que sea el 107 quien lo haga dado que sólo necesita un salto, mientras que si lo hiciera el puente 101 se requerirían dos saltos. Una consideración adicional es que pueden producirse cambios en la configuración, de manera que, por ejemplo, el puente 107 puede fallar, en cuyo caso las tramas siguientes desde la estación 1 hacia la 5 deberían ir a través del puente 101. Por tanto, se puede decir que la capacidad de encaminamiento debe tener en consideración la topología de la configuración de interconexión entre redes y puede requerir ser alterada dinámicamente.

En los últimos años se han propuesto e implementado varias técnicas de encaminamiento. La más sencilla y comúnmente usada es la de **encaminamiento estático**. Esta estrategia resulta adecuada para un número pequeño de redes LAN y para interconexiones relativamente estables. Adicionalmente, dos grupos del comité IEEE 802 han desarrollado especificaciones para estrategias de encaminamiento. El grupo IEEE 802.1 ha propuesto una normalización de encaminamiento basada en el uso del algoritmo del **árbol de expansión** (*spanning tree*), mientras que el comité de anillo con paso de testigo (*token ring*), IEEE 802.5, ha propuesto su propia especificación, denominada **encaminamiento desde el origen** (*source routing*). En el resto de la sección se presentan las estrategias de encaminamiento estático y del árbol de expansión, que es el algoritmo de encaminamiento para puentes más usado.

En el encaminamiento estático se selecciona una ruta para cada pareja de LAN origen-destino en la configuración. Si se dispone de rutas alternativas entre dos LAN, generalmente se selecciona aquella con menor número de saltos. Las rutas son fijas, o al menos sólo cambian cuando se produce un cambio en la topología de la interconexión.

La estrategia para llevar a cabo una configuración de encaminamiento fija para puentes es similar a la empleada en una red de conmutación de paquetes (*véase* Figura 12.3). Se crea una matriz de encaminamiento central, almacenada quizá en un centro de control de red, que indica, para cada pareja de LAN origen-destino, la identidad del primer puente en la ruta. Así, por ejemplo, la ruta desde la LAN E a la LAN F comienza yendo a la LAN A a través del puente 107. Consultando de nuevo la matriz, la ruta desde la LAN A a la F pasa por el puente 102 para alcanzar la LAN C. Finalmente, la ruta desde la LAN C a la LAN F es directa a través del puente 105. Por tanto, la ruta completa desde la LAN E hasta la LAN F es puente 107, LAN A, puente 102, LAN C, puente 105.

Las tablas de encaminamiento se pueden obtener a partir de esta matriz y se guardan en cada puente. Cada puente precisa una tabla para cada una de las LAN a las que está conectado. La información de cada tabla se obtiene a partir de una sola fila de la matriz. Por ejemplo, el puente 105 tiene dos tablas, una para las tramas recibidas de la LAN C y otra para las de la LAN F. La tabla muestra, para cada dirección MAC destino posible, la identidad de la LAN a la que el puente debería enviar la trama.

Una vez establecidas las tablas, el encaminamiento es una tarea sencilla. Un puente copia las tramas procedentes de cada una de sus LAN. Si la dirección MAC de destino corresponde con una entrada de su tabla de encaminamiento, la trama se retransmite a través de la LAN apropiada.

La estrategia de encaminamiento estático se usa ampliamente en los productos comerciales existentes, siendo necesaria la carga manual de las tablas de encaminamiento por parte de un administrador de red. Las principales ventajas de esta estrategia son su sencillez y sus mínimas necesidades de procesamiento. Sin embargo, en una interconexión compleja, en la que los puentes se pueden incorporar dinámicamente y pueden existir fallos, esta estrategia resulta demasiado limitada.

TÉCNICA DEL ÁRBOL DE EXPANSIÓN

El método del árbol de expansión es un mecanismo en el que los puentes desarrollan automáticamente una tabla de encaminamiento y la actualizan en respuesta a cambios en la topología. El algoritmo consta de tres mecanismos: retransmisión de tramas, aprendizaje de direcciones y mecanismo para evitar bucles.

Retransmisión de tramas

En este esquema, un puente mantiene una **base de datos de retransmisión** (*forwarding database*) para cada puerto de conexión a una LAN. La base de datos indica las direcciones de estación para las que las tramas deben transmitirse sobre un puerto dado. Esto se puede interpretar de la siguiente forma: para cada puerto se mantiene una lista de estaciones situadas en el «mismo lado» del puente que el puerto. Por ejemplo, para el puente 102 de la Figura 15.10, las estaciones de las LAN C, F y G se encuentran en el mismo lado del puente que el puerto de la LAN C, y las estaciones de las LAN A, B, D y E están en el mismo lado del puente que el puerto de la LAN A. Cuando se recibe una trama por uno de los puertos, el puente debe decidir si la trama se enviará a través suyo y sobre cuál de los otros puertos se realizará la retransmisión. Suponiendo que un puente recibe una trama MAC a través del puerto *x*, se aplican las siguientes reglas:

1. Búsqueda en la base de datos de retransmisión para determinar si la dirección MAC se asocia a un puerto distinto de *x*.
2. Si no se encuentra la dirección MAC de destino, la trama se envía a través de todos los puertos excepto por el que llegó. Esto es parte de la técnica de aprendizaje que se describe más adelante.
3. Si la dirección de destino se encuentra en la base de datos para algún puerto *y*, se determina si ese puerto se encuentra en estado de bloqueo o de envío. Por razones que se explicarán más adelante, un puerto puede estar a veces bloqueado, lo que le impide emitir o recibir tramas.
4. Si el puerto *y* no está bloqueado, se transmite la trama a través de ese puerto sobre la LAN a la que se encuentra conectado.

Aprendizaje de direcciones

El esquema anterior se basa en la existencia en los puentes de una base de datos de retransmisión que indica la dirección de cada estación destino desde el puente en cuestión. Como en el caso del encaminamiento estático, esta información puede cargarse a priori en el puente. Sin embargo, sería deseable un mecanismo automático efectivo para aprender las direcciones de cada estación. Un esquema sencillo para conseguir esta información se basa en el empleo del campo de dirección origen presente en las tramas MAC.

La estrategia es como sigue. Cuando se recibe una trama por un puerto dado, es evidente que viene desde la dirección de la LAN entrante. El campo de dirección origen de la trama indica la estación emisora, de modo que un puente puede actualizar su base de datos de retransmisión a partir de esa dirección MAC. Con el fin de permitir cambios en la topología, cada entrada en la base de datos dispone de un temporizador. Cuando se añade una nueva entrada a la base de datos, se activa el temporizador asociado. Si éste expira, se elimina la entrada de la base de datos dado que la información de dirección correspondiente puede no ser válida por más tiempo. Cada vez que se recibe una trama se comprueba su dirección origen en la base de datos. Si se encuentra como entrada ya en ésta, se actualiza (la dirección puede haber cambiado) y se reinicia el temporizador. Si la entrada, por el contrario, no está en la base de datos, se crea una nueva con su propio temporizador.

Algoritmo del árbol de expansión

El mecanismo de aprendizaje de direcciones descrito anteriormente es efectivo si la topología de la interconexión de redes es un árbol; es decir, si no existen rutas alternativas en la red. La existencia de rutas alternativas implica la aparición de bucles cerrados. Por ejemplo, la siguiente ruta en la Figura 15.10 es un bucle cerrado: LAN A, puente 101, LAN B, puente 104, LAN E, puente 107, LAN A.

Para analizar el problema creado por la existencia de un bucle cerrado consideremos la Figura 15.11. La estación A transmite una trama destinada a la estación B en el instante de tiempo t_0.

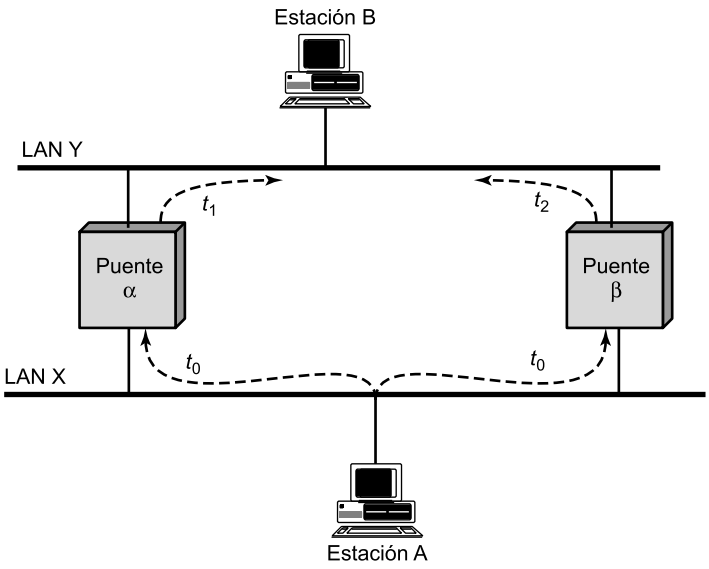


Figura 15.11. Bucle de puentes.

Ambos puentes capturan esta trama y actualizan sus bases de datos para indicar que la estación A se encuentra en la dirección de la LAN X, y retransmiten la trama a través de la LAN Y. Supongamos que el puente α la retransmite en el instante de tiempo t_1 y el puente β un poco después, en t_2. Así, B recibirá dos copias de la trama. Además, cada puente recibirá las transmisiones de los otros a través de la LAN Y. Obsérvese que cada transmisión es una trama MAC con la dirección origen de A y la dirección destino de B, con lo que cada puente actualizará su base de datos para indicar que la estación A se encuentra en la dirección de la LAN Y. Ningún puente es capaz ahora de retransmitir una trama dirigida a la estación A.

Para solucionar este problema se utiliza un sencillo resultado de la teoría de grafos: para cualquier grafo conectado, compuesto de nodos y de terminales que conectan cada par de nodos, existe un árbol de expansión de terminales que mantiene la conectividad del grafo pero no contiene bucles cerrados. En términos de interconexión, cada red LAN se corresponde con un nodo del grafo y cada puente con una arista. Así, en la Figura 15.10, la eliminación de uno (y sólo uno) de los puentes 107, 101 y 104 da lugar a un árbol de expansión. Resulta deseable el desarrollo de un algoritmo sencillo mediante el que los puentes de la interconexión puedan intercambiar información suficiente (sin intervención de los usuarios) para obtener el árbol de expansión. El algoritmo debe ser dinámico; es decir, los puentes deben ser capaces de percatarse ante un cambio en la topología y obtener automáticamente un nuevo árbol de expansión.

El algoritmo del árbol de expansión desarrollado por IEEE 802.1, como su propio nombre sugiere, puede desarrollar dicho árbol de expansión. Todo lo que se precisa es que cada uno de los puentes tenga asignado un identificador único y se asocien costes a cada uno de los puertos de los puentes. Aparte de cualquier consideración especial, todos los costes podrían ser iguales, lo que produciría un árbol de menor número de saltos. El algoritmo implica el intercambio de un número reducido de mensajes entre todos los puentes para obtener el árbol de expansión de mínimo coste. Cuando se produzca un cambio en la topología, los puentes recalcularán automáticamente el árbol de expansión.

15.5. CONMUTADORES DE LA CAPA 2 Y LA CAPA 3

Recientemente se ha producido una proliferación de diversos tipos de dispositivos utilizados para la interconexión de redes LAN que van más allá de los puentes que se discutieron en la Sección 15.4 y los dispositivos de encaminamiento que son tratados en la Parte V. Estos dispositivos pueden ser clasificados en dos categorías: conmutadores de la capa 2 y conmutadores de la capa 3. Comenzaremos exponiendo algunas cuestiones relativas a los conmutadores antes de profundizar en ambos tipos.

CONCENTRADORES

Anteriormente se ha utilizado el término *concentrador* en el contexto de una LAN con topología en estrella. El concentrador es un elemento activo que actúa como elemento central de la estrella. Cada estación se conecta al concentrador mediante dos enlaces (transmitir y recibir). El concentrador actúa como un repetidor: cuando transmite una única estación, el concentrador replica la señal en la línea de salida hacia cada estación. Generalmente, el enlace consiste en dos pares trenzados no apantallados. Dada la alta velocidad y la baja calidad de transmisión del par trenzado no apantallado, la longitud de un enlace está limitada a en torno a 100 m. Como alternativa, se puede usar un enlace de fibra óptica, en cuyo caso la longitud máxima es del orden de 500 m.

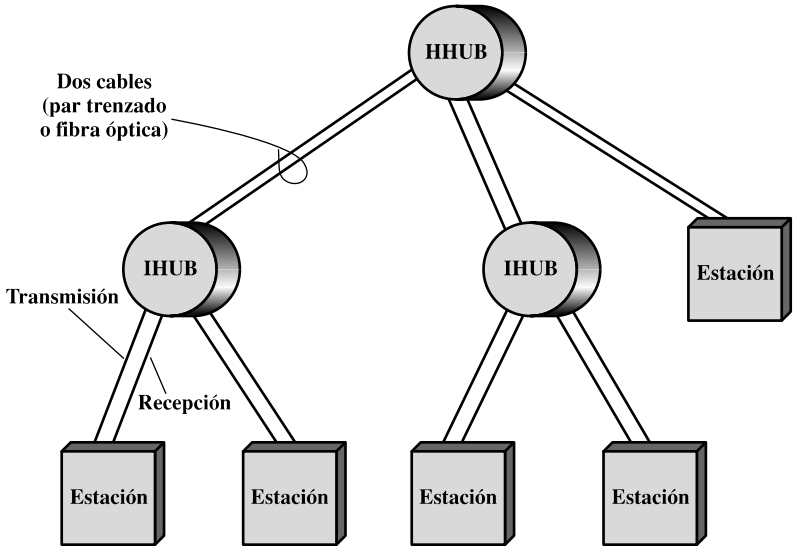


Figura 15.12. Topología en estrella en dos niveles.

Obsérvese que, aunque este esquema es físicamente una estrella, funciona lógicamente como un bus: una transmisión por parte de una estación se recibe en el resto de estaciones y se produce colisión si dos estaciones transmiten al mismo tiempo.

Varios niveles de concentradores se pueden poner en cascada formando una configuración jerárquica. En la Figura 15.12 se muestra una configuración en dos niveles. Existe un **concentrador raíz** (HHUB, *Header Hub*) y uno o más **concentradores intermedios** (IHUB, *Intermediate Hub*). Cada concentrador puede ser una mezcla de estaciones y otros concentradores conectados a él por debajo. Esta estructura se adecúa bien a edificios cableados, donde, generalmente, existe un armario de interconexiones en cada planta del edificio, pudiendo colocarse un concentrador en cada una de ellas. Cada concentrador podría dar servicio a las estaciones situadas en su misma planta.

CONMUTADORES DE LA CAPA 2

Un dispositivo, denominado conmutador de la capa 2, o simplemente conmutador, ha desplazado en popularidad a los concentradores en los últimos años, especialmente en el contexto de las redes LAN de alta velocidad.

Para aclarar la distinción entre concentradores y conmutadores, en la Figura 15.13a se muestra un bus típico correspondiente a una LAN convencional a 10 Mbps. Un bus se instala de forma que todos los dispositivos a conectar se encuentran próximos a él. En la figura, la estación B está transmitiendo, de forma que esta transmisión sale de B hacia el bus, a lo largo de éste en los dos sentidos y sobre las líneas de acceso de cada una de las otras estaciones conectadas. En esta configuración, todas las estaciones deben compartir la capacidad total del bus, que es de 10 Mbps.

Un concentrador, normalmente situado en un armario de cableado del edificio, emplea una estructura en estrella para conectar las estaciones al mismo, de forma que la transmisión por parte una estación se recibe en el concentrador y se retransmite sobre todas las líneas de salida. Por tanto, para evitar la ocurrencia de colisión, sólo una estación puede transmitir en un momento dado. De nuevo, la capacidad total de la LAN es de 10 Mbps. El uso de un concentrador presenta varias

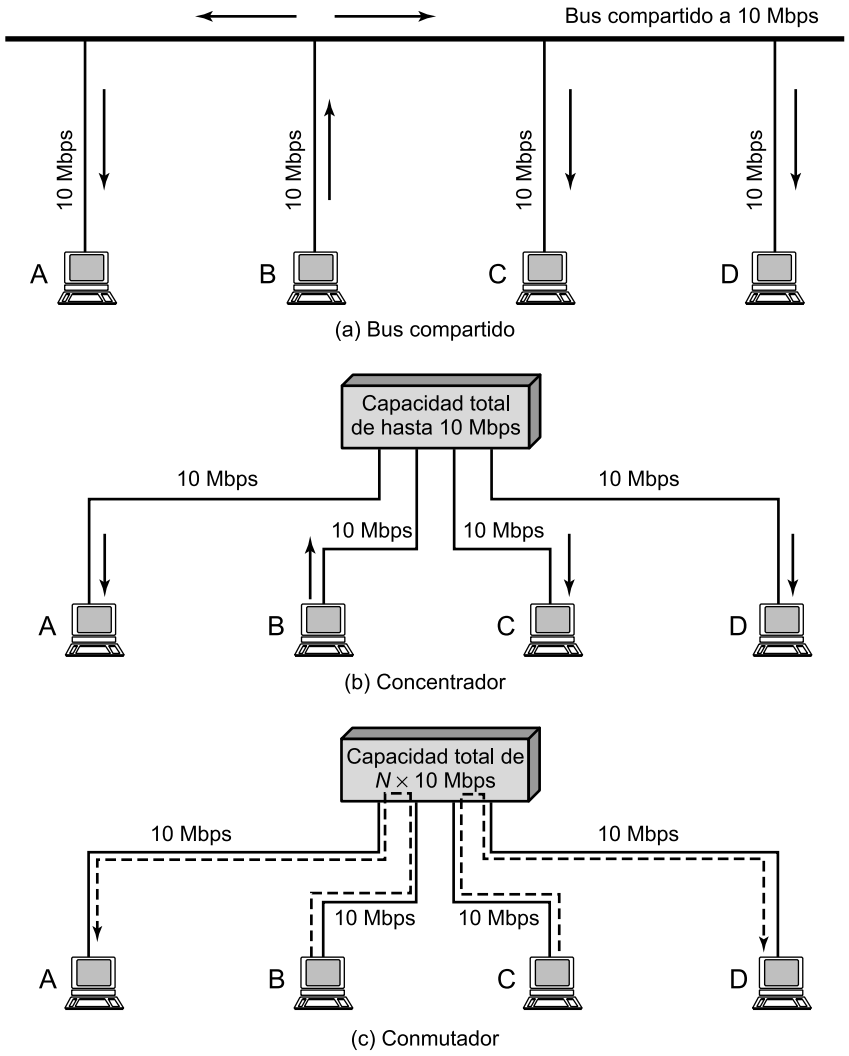


Figura 15.13. Conmutadores y concentradores en una LAN.

ventajas frente a la configuración en bus: aprovecha el cableado de los edificios, además del hecho de que el concentrador se puede configurar para determinar el mal funcionamiento de una estación que congestiona la red, de modo que se podría eliminar dicha estación de la red. En la parte (b) de la figura se ilustra el funcionamiento de un concentrador. De nuevo se encuentra transmitiendo la estación B. La transmisión sale de B a lo largo de la línea de transmisión entre esta estación y el concentrador, y desde él al resto de estaciones conectadas a lo largo de las líneas de recepción correspondientes.

Se pueden mejorar las prestaciones mediante el uso de un conmutador de la capa 2. En este caso, el centro raíz actúa como un conmutador, de forma análoga a un conmutador de paquetes o de circuitos. Una trama procedente de una estación dada es conmutada hacia la correspondiente línea de salida para su envío hacia la estación destino. Al mismo tiempo, algunas otras líneas desocupadas se pueden usar para conmutar otro tráfico. En la Figura 15.13c se muestra un ejemplo en

el que la estación B está transmitiendo una trama a A y, al mismo tiempo, C transmite una trama hacia D. Así, en este ejemplo, el rendimiento actual de la LAN es 20 Mbps, aunque cada dispositivo individual esté limitado a 10 Mbps. El conmutador de la capa 2 presenta varias características interesantes:

1. No se necesita cambiar el software ni el hardware de los dispositivos conectados para convertir una LAN en bus o una LAN con un concentrador en una LAN con un conmutador. En el caso de una LAN Ethernet, cada dispositivo conectado continúa usando el protocolo CSMA/CD para acceder a la LAN. Desde el punto de vista de los dispositivos conectados nada ha cambiado en el acceso lógico.

2. Suponiendo que el conmutador tiene suficiente capacidad para atender a todos los dispositivos conectados, cada uno de ellos tiene una capacidad dedicada igual a la de la LAN original completa. Por ejemplo, en la Figura 15.13c, si el conmutador puede dar un rendimiento de 20 Mbps, parece como si cada dispositivo conectado tuviese una capacidad dedicada de entrada o salida de 10 Mbps.

3. El conmutador de la capa 2 permite el escalado de forma sencilla, pudiéndose conectar dispositivos adicionales a él mediante el incremento correspondiente de su capacidad.

Comercialmente existen dos tipos de centros conmutados:

- **Conmutador de almacenamiento y envío (*store-and-forward switch*):** el conmutador acepta una trama sobre una línea de entrada, la almacena temporalmente y después la encamina hacia la línea de salida correspondiente.

- **Conmutador rápido (*cut-through switch*):** el conmutador aprovecha que la dirección de destino se encuentra al comienzo de la trama MAC (control de acceso al medio) para retransmitir la trama entrante sobre la línea de salida correspondiente tan pronto como sabe la dirección de destino.

El conmutador de tipo rápido permite el mayor rendimiento posible, aunque a riesgo de propagar tramas erróneas dado que no es capaz de comprobar el campo CRC antes de efectuar la retransmisión. Por su parte, el conmutador de almacenamiento y envío implica un retardo entre la emisión y la recepción, pero mantiene la integridad completa de la red.

Un conmutador de la capa 2 puede ser visto como una versión *full-duplex* de un concentrador, pudiendo incorporar además la lógica necesaria para funcionar como un puente multipunto. En [BREY99] se enumeran las siguientes diferencias entre puentes y conmutadores de la capa 2:

- La gestión de las tramas en un puente se hace por software, mientras que un conmutador de la capa 2 lleva a cabo el reconocimiento de direcciones y el reenvío de tramas por hardware.

- Por lo general, un puente sólo puede analizar y retransmitir las tramas de una en una, mientras que un conmutador de la capa 2 tiene varias rutas de datos que actúan en paralelo, pudiendo así manejar múltiples tramas simultáneamente.

- Un puente utiliza siempre un mecanismo de almacenamiento y envío, mientras que un conmutador de la capa 2 puede funcionar en modo rápido (*cut-through*).

Los puentes han sufrido un receso comercial debido a las mayores prestaciones ofrecidas por los conmutadores y a que éstos pueden realizar sus mismas funciones. Las nuevas instalaciones suelen incluir un conmutador de capa 2 que efectúa las funciones de un puente, en lugar de un puente.

CONMUTADORES DE LA CAPA 3

Los conmutadores de capa 2 ofrecen unas prestaciones adecuadas para satisfacer los elevados requisitos de tráfico generado por computadores personales, estaciones de trabajo y servidores. No obstante, a medida que el número de dispositivos en un edificio o conjunto de ellos crece, los conmutadores de capa 2 muestran algunas deficiencias. Presentan, en particular, dos problemas fundamentales: sobrecarga de difusión y falta de enlaces múltiples.

Un conjunto de dispositivos y redes LAN conectados por un conmutador de capa 2 posee un espacio de direccionamiento plano. El término *plano* hace referencia al hecho de que todos los usuarios comparten una dirección de difusión común. De esta forma, si un dispositivo cualquiera emite una trama MAC con una dirección de difusión, la trama será entregada a todos los dispositivos conectados a cualquier segmento de la red interconectado por conmutadores de capa 2 y/o puentes. En una red grande, una tasa de tramas de difusión elevada puede crear una sobrecarga tremenda. Se puede dar un caso aún peor, conocido como *tormenta de difusión*: un dispositivo defectuoso que inserte continuamente tramas de difusión llega a congestionar completamente la red.

El segundo problema de rendimiento concerniente al uso de puentes y/o conmutadores de capa 2 está relacionado con el hecho de que las normativas en vigor prohíben la existencia de bucles cerrados en la red. Dicho de otro modo, sólo puede existir un único camino entre cualesquiera dos dispositivos. Esto impide que cualquier implementación que se adecue a los estándares proporcione múltiples caminos entre dispositivos, limitando así tanto el rendimiento como la fiabilidad de la red.

Una estrategia lógica para hacer frente a estas limitaciones consiste en dividir una red local grande en una serie de **subredes** conectadas entre sí por dispositivos de encaminamiento (*routers*). Así, una trama MAC de difusión queda restringida únicamente a aquellos dispositivos y conmutadores que pertenecen a la misma subred. Además, los dispositivos de encaminamiento basados en IP emplean algoritmos de encaminamiento sofisticados que toleran la existencia de varios caminos entre subredes a través de diferentes dispositivos de encaminamiento.

Sin embargo, el uso de dispositivos de encaminamiento para hacer frente a las desventajas de los puentes y conmutadores de capa 2 presenta problemas de rendimiento, puesto que, por lo general, los dispositivos de encaminamiento realizan todo el procesamiento IP relacionado con la retransmisión por software. Las redes LAN de alta velocidad y los conmutadores de altas prestaciones pueden bombear del orden de millones de paquetes por segundo, mientras que un dispositivo de encaminamiento basado en software puede manejar por debajo de un millón de paquetes por segundo. Para satisfacer estos requisitos de carga, algunos fabricantes han desarrollado dispositivos de encaminamiento que implementan la lógica de retransmisión de paquetes en hardware.

Existen diversos esquemas de conmutadores de capa 3 en el mercado, aunque, en términos generales, todos pueden ser clasificados en dos categorías: de tipo paquete a paquete o basados en flujos. Un conmutador tipo paquete a paquete funciona de forma idéntica a un dispositivo de encaminamiento tradicional. Dado que la lógica de retransmisión está en el hardware, el conmutador puede incrementar en un orden de magnitud el rendimiento, en comparación con un dispositivo de encaminamiento que lo haga por software. Un conmutador basado en flujos trata de mejorar el rendimiento mediante la identificación de flujos de paquetes IP que poseen las mismas direcciones de origen y de destino. Esta tarea puede realizarse observando el tráfico de salida, o bien utilizando una etiqueta de flujo en la cabecera de cada paquete (existente en IPv6 pero no en IPv4). Una vez que un flujo es identificado, es posible establecer una ruta predefinida a través de la red para acele-

rar el proceso de retransmisión. De esta forma se consigue un incremento en el rendimiento con respecto a un dispositivo de encaminamiento puramente basado en software.

La Figura 15.14 es un ejemplo típico de la solución adoptada en una organización con un número elevado de computadores personales y estaciones de trabajo (de miles a decenas de miles). Los sistemas de escritorio tienen enlaces de 10 Mbps a 100 Mbps dentro de una LAN controlada por un conmutador de capa 2. Es más que probable, además, la existencia de conectividad proporcionada por una red LAN inalámbrica para usuarios móviles. Los conmutadores de capa 3 constituyen el núcleo de las redes locales, formando así una red troncal. Estos conmutadores suelen estar interconectados entre sí por enlaces de 1 Gbps, estando conectados a los conmutadores de capa 2 por enlaces con velocidades que oscilan entre 100 Mbps y 1 Gbps. Los servidores se conectan directamente a los conmutadores de capa 2 o capa 3 a 1 Gbps o, posiblemente, a 100 Mbps. Un dispositivo de encaminamiento de más bajo coste y basado en software proporciona la conexión con una WAN. Los círculos en la figura señalan subredes LAN diferentes, de tal forma que una trama MAC de difusión queda limitada a su propia subred.

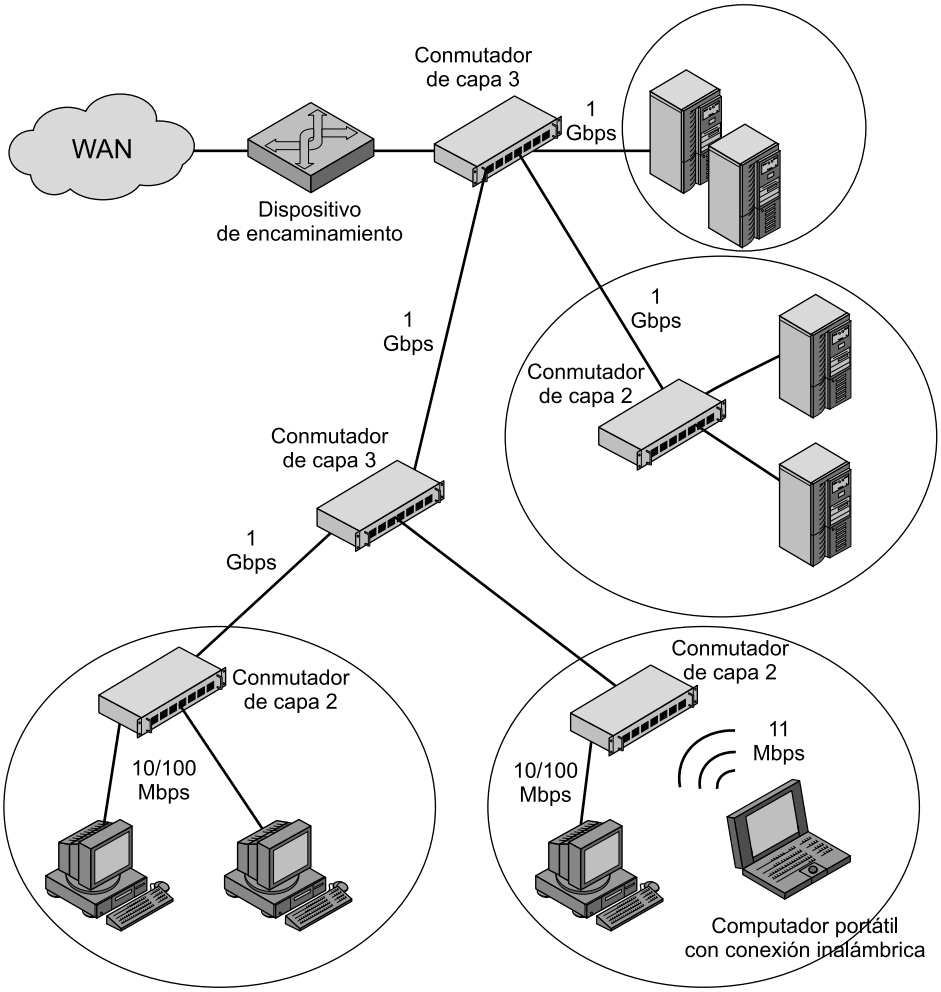


Figura 15.14. Configuración de red típica en oficinas.

15.6. LECTURAS Y SITIOS WEB RECOMENDADOS

El material de este capítulo se cubre con mucha mayor profundidad en [STAL00]. [METZ99] proporciona un tratamiento excelente de los conmutadores de capa 2 y capa 3, con una discusión detallada de productos y estudio de casos. Otra referencia interesante es [SEIF00].

METZ99 Metzler, J., y DeNoia, L. *Layer 2 Switching*. Upper Saddle River, NJ: Prentice Hall, 1991.

SEIF00 Seifert, R. *The Switch Book*. New York: Wiley, 2000.

STAL00 Stallings, W. *Local and Metropolitan Area Networks, 6th ed.* Upper Saddle River, NJ: Prentice Hall, 2000.

SITIO WEB RECOMENDADO

- **Comité de normalización LAN/MAN IEEE 802**: estado y documentos de todos los grupos de trabajo.

15.7. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

árbol de expansión
concentrador
control de acceso al medio (MAC)
control de enlace lógico
conmutador
conmutador de capa 2
conmutador de capa 3
puente
red de área local (LAN)
red de almacenamiento (SAN)
topología en anillo
topología en árbol
topología en bus
topología en estrella

CUESTIONES DE REPASO

15.1. ¿Qué diferencias hay entre los requisitos clave para las redes existentes en salas de computadores de aquellos necesarios para redes de área local de computadores personales?

15.2. ¿Qué diferencias hay entre una red LAN de respaldo, una red SAN y una red LAN troncal?

15.3. ¿Qué es la topología de una red?

15.4. Enumere cuatro topologías comunes para redes LAN y describa brevemente su principio de funcionamiento.

15.5. ¿Cuál es el propósito del comité IEEE 802?

15.6. ¿Por qué existen diferentes normativas para redes LAN?

15.7. Enumere y describa brevemente los servicios proporcionados por LLC.

15.8. Enumere y describa brevemente los modos de operación proporcionados por el protocolo LLC.

15.9. Enumere algunas funciones básicas que se realicen en la capa MAC.

15.10. ¿Qué funciones lleva a cabo un puente?

15.11. ¿Qué es un árbol de expansión?

15.12. ¿Qué diferencias existen entre un concentrador y un conmutador de capa 2?

15.13. ¿Cuál es la diferencia entre un conmutador de almacenamiento y envío y uno rápido?

EJERCICIOS

15.1. ¿Se podría usar HDLC como protocolo de control de enlace de datos en una LAN en lugar de LLC? ¿Por qué?

15.2. Un dispositivo asíncrono, como por ejemplo un teletipo, transmite caracteres uno a uno con retardos impredecibles entre ellos. ¿Qué problemas pueden aparecer, si es que hay alguno, si un dispositivo así se conecta a una red local y se le permite transmitir a voluntad (sujeto a conseguir el acceso al medio)? ¿Cómo se podrían solucionar estos problemas?

15.3. Considere la transferencia de un fichero que contiene un millón de caracteres de 8 bits desde una estación a otra. Indique el tiempo consumido y el rendimiento efectivo para los siguientes casos:

a) Una topología en estrella con conmutación de circuitos. Suponga que el tiempo de establecimiento de llamada es despreciable y que la velocidad de transmisión del medio es 64 kbps.

b) Una topología en bus con dos estaciones distanciadas D, una velocidad de transmisión de B bps y un tamaño de paquete P con 80 bits suplementarios. Cada paquete se confirma mediante un paquete de 88 bits antes de que se envíe el siguiente. La velocidad de propagación en el bus es de 200 m/μs. Resuelva para:

(1) $D = 1$ km, $B = 1$ Mbps, $P = 256$ bits

(2) $D = 1$ km, $B = 10$ Mbps, $P = 256$ bits

(3) $D = 10$ km, $B = 1$ Mbps, $P = 256$ bits

(4) $D = 1$ km, $B = 50$ Mbps, $P = 10.000$ bits

c) Una topología en anillo con una longitud circular total de $2D$, con una distancia D entre las dos estaciones. La confirmación se realiza permitiendo a la estación destino dejar pasar los paquetes hacia la estación origen estableciendo un bit de confirmación. Existen N repetidores en el anillo, cada uno de los cuales introduce un retardo igual al tiempo de duración de un bit. Repita el cálculo para cada una de las situaciones (1) a (4) del apartado anterior para $N = 10$, 100 y 1.000.

15.4. Considere un bus en banda base con varias estaciones equidistantes con una velocidad de transmisión de 10 Mbps y una longitud del bus de 1 km.

a) ¿Cuál es el tiempo medio para enviar una trama de 10.000 bits a otra estación, medido desde el comienzo de la transmisión hasta el final de la recepción? Suponga una velocidad de propagación de 200 m/μs.

b) Si dos estaciones comienzan a transmitir exactamente al mismo tiempo, sus paquetes interferirán entre sí. Si cada estación transmisora monitoriza el bus durante la trans-

misión, ¿cuánto tiempo tarda, en segundos, en percatarse de la ocurrencia de una interferencia? ¿Y en intervalos de duración de un bit?

15.5. Repita el Ejercicio 15.4 para una velocidad de transmisión de 100 Mbps.

15.6. Para una velocidad de propagación de 200 m/μs, ¿cuál es la longitud efectiva añadida a un anillo para un retardo de bit en cada repetidor de:

a) 1 Mbps?

b) 40 Mbps?

15.7. Para unir dos edificios se utiliza una topología en árbol. Si se puede conseguir el permiso para colocar el cable entre los dos edificios, se utiliza un esquema de árbol continuo. En caso contrario, cada edificio tendrá una red de topología en árbol independiente y un enlace punto a punto conectará una estación de comunicaciones especial en una red con una estación de comunicaciones en la otra red. ¿Qué funciones deben realizar las estaciones de comunicaciones? Repita el proceso para un anillo y una estrella.

15.8. Un sistema A consiste en un anillo simple con 300 estaciones, una por repetidor. Un sistema B consta de tres anillos con 100 estaciones cada uno unidos por un puente. Si la probabilidad de fallo en un enlace es P_1, en un repetidor es P_r y en un puente es P_b, obtenga una expresión para:

a) probabilidad de fallo del sistema A.

b) probabilidad de fallo completo del sistema B.

c) probabilidad de que una estación particular no encuentre disponible la red, para los sistemas A y B.

d) probabilidad de que dos estaciones cualquiera, elegidas aleatoriamente, no puedan comunicarse, para los sistemas A y B.

e) calcule los valores para los apartados (a) a (d) con $P_1 = P_b = P_r = 10^{-2}$.

15.9. Dibuje una figura similar a la Figura 15.9 para una configuración en la que:

a) se conectan dos redes LAN a través de dos puentes conectados mediante un enlace punto a punto.

b) se conectan dos LAN a través de dos puentes conectados mediante una red de conmutación de paquetes X.25.

15.10. Especifique la matriz de encaminamiento central y las tablas de encaminamiento de cada uno de los puentes de la configuración dada en la Figura 15.10.

CAPÍTULO 16

Redes LAN de alta velocidad

16.1. Surgimiento de las redes LAN de alta velocidad

16.2. Ethernet
Control de acceso al medio en IEEE 802.3
Especificaciones IEEE 802.3 10 Mbps (Ethernet)
Especificaciones IEEE 802.3 100 Mbps (Fast Ethernet)
Gigabit Ethernet
Ethernet de 10 Gpbs

16.3. Anillo con paso de testigo
Funcionamiento del anillo
Control de acceso al medio
Opciones de medios de transmisión en IEEE 802.5

16.4. Canal de fibra
Elementos del canal de fibra
Arquitectura de protocolos del canal de fibra
Medios físicos y topologías del canal de fibra
Perspectivas del canal de fibra

16.5. Lecturas y sitios web recomendados

16.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

Apéndice 16A. Codificación de señales digitales para redes LAN
4B/5B-NRZI
MLT-3
8B6T
8B/10B

Apéndice 16B. Análisis de prestaciones
Efecto del retardo de propagación y la velocidad de transmisión
Modelos sencillos de eficiencia para las técnicas de paso de testigo y CSMA/CD

CUESTIONES BÁSICAS

- El estándar IEEE 802.3, conocido como Ethernet, comprende actualmente velocidades de datos de 10 Mbps, 100 Mbps, 1Gbps y 10 Gbps. En el caso de las velocidades más bajas se utiliza el protocolo MAC CSMA/CD, mientras que a 1 Gbps y 10 Gbps se emplea una técnica de conmutación.
- El estándar de paso de testigo IEEE 802.5 ofrece velocidades de datos desde 4 Mbps hasta 1 Gbps.
- El canal de fibra es una red conmutada de nodos diseñada para proporcionar enlaces de alta velocidad para aplicaciones como las redes de almacenamiento.

Los años recientes han sido testigos de cambios vertiginosos en aspectos como la tecnología, el diseño y las aplicaciones comerciales de las redes de área local (LAN, *Local Area Network*). Una de las principales características de esta evolución es la introducción de toda una gama de nuevos esquemas en las redes locales de alta velocidad. Los distintos enfoques para el diseño de redes LAN de alta velocidad se han plasmado en productos comerciales con objeto de dar solución a las continuas necesidades del mercado. De entre ellas, las más importantes son:

- **Fast Ethernet y Gigabit Ethernet:** la extensión de la técnica de acceso múltiple con detección de portadora y detección de colisiones de 10 Mbps (CSMA/CD, *Carrier Sense Multiple Access with Collision Detection*) a altas velocidades constituye una estrategia lógica, puesto que tiende a preservar la inversión realizada en los sistemas actuales.
- **Canal de fibra:** este estándar proporciona una solución de bajo coste y fácilmente escalable para alcanzar tasas de datos elevadas en áreas locales.
- **Redes LAN inalámbricas de alta velocidad:** la tecnología y estándares de redes LAN inalámbricas han alcanzado por fin madurez y las normativas y productos de alta velocidad están siendo introducidos.

La Tabla 16.1 enumera algunas de las características de estos enfoques. El contenido restante de este capítulo aborda en mayor profundidad los detalles concernientes a Ethernet, canal de fibra y anillo con paso de testigo. Por su parte, las redes LAN inalámbricas serán tratadas en el Capítulo 17.

Tabla 16.1. Características de algunas redes LAN de alta velocidad.

	Fast Ethernet	Gigabit Ethernet	Canal de fibra	LAN inalámbrica
Velocidad de datos	100 Mbps	1 Gbps, 10 Gbps	100 Mbps-3,2 Gbps	1 Mbps-54 Mbps
Medio de transmisión	UTP, STP, fibra óptica	UTP, cable apantallado fibra óptica	Fibra óptica cable coaxial, STP	Microondas 2,4 GHz, 5 GHz
Método de acceso	CSMA/CD	Conmutado	Conmutado	CSMA/Sondeo
Estándar	IEEE 802.3	IEEE 802.3	Asociación del canal de fibra	IEEE 802.11

16.1. SURGIMIENTO DE LAS REDES LAN DE ALTA VELOCIDAD

Los computadores personales y las estaciones de trabajo comenzaron a recibir una amplia aceptación en los entornos comerciales a principios de la década de los ochenta, habiendo alcanzado actualmente un estatus similar al del teléfono: una herramienta esencial en cualquier oficina. Hasta hace relativamente poco, las redes LAN en las oficinas proporcionaban servicios básicos de conectividad (conexión de computadores personales y terminales a grandes servidores y estaciones que ejecutaban aplicaciones corporativas) y ofrecían una conectividad para trabajo en grupo entre departamentos o divisiones. Los patrones de tráfico en ambos casos presentaban una carga relativamente baja, estando principalmente influenciados por la transferencia de ficheros y de correo electrónico. Las redes que se encontraban disponibles para este tipo de carga, principalmente Ethernet y anillo con paso de testigo, se ajustaban satisfactoriamente a tales entornos.

En los últimos años se han manifestado dos tendencias significativas que han alterado el papel que desempeñan los computadores personales y, por tanto, los requisitos de las redes LAN:

- La velocidad y potencia de cálculo de los computadores personales ha continuado disfrutando de un crecimiento explosivo. Actualmente, las plataformas más potentes soportan aplicaciones con un alto contenido en gráficos e incluso sistemas operativos con una interfaz gráfica de usuario muy elaborada.
- Las organizaciones de gestión de sistemas de información han reconocido las redes LAN no sólo como una tecnología viable sino también esencial, promoviendo así el trabajo en red. Esta tendencia comenzó con el paradigma cliente/servidor, que se ha convertido en la arquitectura dominante en los entornos de negocio y, más recientemente, en las redes privadas. Estos dos enfoques implican transferencias frecuentes de volúmenes de datos potencialmente grandes en un entorno orientado a transacciones.

El efecto de estas tendencias ha sido el incremento del volumen de datos que debe ser manejado por las redes LAN y, dado que las aplicaciones son más interactivas, una reducción del retardo aceptable en las transferencias. La primera generación de Ethernet de 10 Mbps y anillo con paso de testigo de 16 Mbps simplemente no fueron diseñadas para dar cabida a estos requisitos.

Los siguientes ejemplos ilustran algunos entornos que requieren redes LAN de alta velocidad:

- **Agrupación centralizada de servidores:** en muchas aplicaciones existe la necesidad de que los sistemas cliente sean capaces de recuperar cantidades enormes de datos de un conjunto centralizado de servidores (*server farm*). Un ejemplo lo constituyen las aplicaciones de publicación de contenidos en color, en las que los servidores contienen generalmente decenas de gigabytes de imágenes que deben ser descargadas a las estaciones de dibujo. A medida que el rendimiento de los servidores se incrementa, el cuello de botella se ha ido desplazando hacia la red. Una Ethernet conmutada no resolvería este problema debido al límite de 10 Mbps por enlace hacia el cliente.
- **Grupos de trabajo con altos requisitos:** estos grupos constan generalmente de un número reducido de usuarios que cooperan entre sí y que mueven archivos masivos de datos a lo largo de la red. Algunos ejemplos son los grupos de desarrollo de software que ejecutan comprobaciones sobre una versión nueva de un software, o una compañía de diseño asistido por computador (CAD) que ejecuta regularmente simulaciones de los nuevos diseños. En estos casos existe una gran cantidad de datos que es distribuida a varias estaciones de trabajo, procesada en las mismas y devuelta de nuevo a una alta velocidad, repitiéndose iterativamente este proceso.

- **Red troncal local de alta velocidad:** a medida que las demandas de capacidad de procesamiento crecen, las redes LAN proliferan en una entidad y se hace cada vez más necesario proporcionar una interconexión de alta velocidad entre ellas.

16.2. ETHERNET

Las redes LAN de alta velocidad más ampliamente utilizadas en la actualidad son las basadas en Ethernet, desarrolladas por el comité de estándares IEEE 802.3. Al igual que sucede con otros estándares de redes LAN, existe una capa de control de acceso al medio y una capa física las cuales se estudian a continuación.

CONTROL DE ACCESO AL MEDIO EN IEEE 802.3

El funcionamiento de la técnica CSMA/CD se puede entender más fácilmente si primero se estudian los esquemas a partir de los que evolucionó.

Precursores

La técnica CSMA/CD y sus precursoras pueden ser denominadas de acceso aleatorio o de contención. Se denominan de acceso aleatorio en el sentido de que no existe un tiempo preestablecido o predecible para que las estaciones transmitan, sino que las transmisiones se organizan aleatoriamente. Son de contención en el sentido de que las estaciones compiten para conseguir el acceso al medio.

La primera de estas técnicas, conocida como ALOHA, se desarrolló para redes de paquetes de radio, siendo, a pesar de ello, aplicable a cualquier medio de transmisión compartido. ALOHA, o ALOHA puro, como también es denominado algunas veces, permite que una estación transmita una trama siempre que lo necesite. A continuación la estación pasa a escuchar el medio durante un tiempo igual al máximo retardo de propagación posible de ida y vuelta a través de la red (igual a dos veces el tiempo de propagación de una trama entre las dos estaciones más separadas) más un pequeño incremento fijo de tiempo. Se considerará que todo ha ido bien si durante este intervalo de escucha la estación oye una confirmación; en caso contrario, retransmitirá la trama. La estación desistirá si no recibe una confirmación después de varias retransmisiones. Una estación receptora determina si una trama recibida es correcta examinando el campo de la secuencia de comprobación de la trama, al igual que se hace en HDLC. Si la trama es válida y la dirección de destino en la cabecera de la trama coincide con la de la receptora, la estación devuelve inmediatamente una confirmación. La trama puede ser incorrecta debido a la presencia de ruido en el canal o debido a que otra estación transmitiera una trama casi al mismo tiempo. En este último caso, las dos tramas pueden interferir entre sí en el receptor, de modo que no se acepte ninguna; esto se conoce como **colisión**. Si se decide que la trama recibida no es válida, la estación receptora simplemente ignorará la trama.

ALOHA es una técnica extremadamente sencilla, debido a lo cual presenta algunos puntos débiles. Dado que el número de colisiones crece rápidamente cuando aumenta la carga, la utilización máxima del canal es sólo del orden del 18 por ciento.

Con objeto de mejorar la eficiencia se desarrolló una modificación sobre ALOHA, conocida como ALOHA ranurado. En este esquema el tiempo del canal se hace discreto, considerando ranu-

ras uniformes de duración igual al tiempo de transmisión de una trama. Para este fin es necesario el uso de un reloj central u otra técnica que permita sincronizar todas las estaciones. La transmisión sólo se permite en los instantes de tiempo que coincidan con el comienzo de una ranura. Así, las tramas que se solapen lo harán completamente, lo que incrementa la utilización máxima del sistema hasta el 37 por ciento aproximadamente.

Tanto ALOHA como ALOHA ranurado presentan una utilización baja del canal. Ninguna de las dos técnicas aprovecha una de las propiedades más importantes en las redes de paquetes de radio y redes LAN, consistente en que el retardo de propagación entre las estaciones es generalmente muy pequeño en comparación con el tiempo de transmisión de las tramas. Consideremos las siguientes observaciones. Si el tiempo de propagación entre estaciones fuese grande en comparación con el tiempo de transmisión, entonces, tras la transmisión de una trama deberá transcurrir mucho tiempo antes de que otras estaciones constaten este hecho. Una de las otras estaciones puede transmitir una trama durante ese intervalo de tiempo, de modo que las dos tramas pueden interferir entre sí y no se aceptará ninguna de ellas. De hecho, si las distancias son suficientemente grandes, pueden comenzar a transmitir varias estaciones una tras otra, y ninguna de sus tramas resultará ilesa. Supongamos, sin embargo, que el tiempo de propagación es pequeño comparado con el de transmisión. En este caso, cuando una estación transmita una trama, el resto de estaciones lo sabrá casi inmediatamente. De esta manera, si pueden constatar esta circunstancia de algún modo, no intentarán transmitir hasta que lo haya hecho la primera. Las colisiones no serán habituales, ya que sólo ocurrirán cuando dos estaciones comiencen a transmitir casi simultáneamente. Otra forma de verlo es que un tiempo de retardo pequeño proporciona a las estaciones una mejor realimentación sobre el estado de la red; esta información se puede usar para mejorar la eficiencia.

Estas observaciones condujeron al desarrollo de la técnica de acceso múltiple con detección de portadora (CSMA, *Carrier Sense Multiple Access*). Con CSMA, una estación que desee transmitir escuchará primero el medio para determinar si existe alguna otra transmisión en curso (detección de portadora). Si el medio está siendo usado, la estación deberá esperar. En cambio, si éste se encuentra libre, la estación podrá transmitir. Puede suceder que dos o más estaciones intenten transmitir aproximadamente al mismo tiempo, en cuyo caso se producirá colisión: los datos de ambas transmisiones interferirán y no se recibirán con éxito. Para solucionar esto, las estaciones aguardan una cantidad de tiempo razonable después de transmitir en espera de una confirmación, teniendo en consideración el retardo de propagación máximo del trayecto de ida y vuelta y el hecho de que la estación que confirma debe competir también por conseguir el medio para responder. Si no llega la confirmación, la estación supone que se ha producido una colisión y retransmite.

Podemos ver cómo esta estrategia resulta efectiva para redes en las que el tiempo de transmisión de trama es mucho mayor que el de propagación. Las colisiones sólo se producirán en el caso de que más de un usuario comience a transmitir dentro del mismo intervalo de tiempo (igual al periodo de propagación). Si una estación comienza a transmitir una trama y no existen colisiones durante el tiempo de propagación que transcurre desde el inicio de la transmisión del paquete hasta que alcanza a la estación más lejana, no se producirá colisión para esta trama dado que ahora todas las estaciones están enteradas de la transmisión.

La utilización máxima que se puede conseguir haciendo uso de CSMA puede superar con mucho la de ALOHA ranurado. La utilización máxima depende de la longitud de la trama y del tiempo de propagación; cuanto mayor sea la longitud de las tramas o cuanto menor sea el tiempo de propagación, mayor será la utilización.

En CSMA se precisa de un algoritmo que determine qué debe hacer una estación si encuentra el medio ocupado. Tres enfoques para resolver este problema se describen en la Figura 16.1. En el

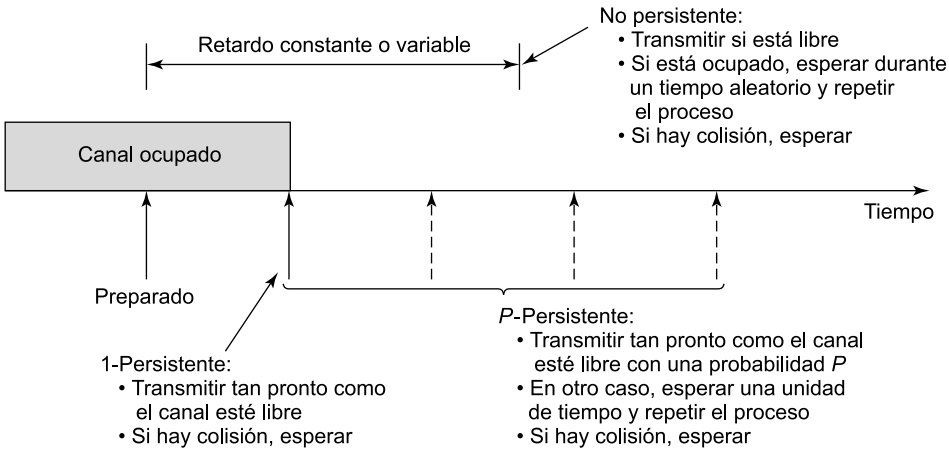

Retardo constante o variable
No persistente:
• Transmitir si está libre
• Si está ocupado, esperar durante un tiempo aleatorio y repetir el proceso
• Si hay colisión, esperar
Canal ocupado
Tiempo
Preparado
1-Persistente:
• Transmitir tan pronto como el canal esté libre
• Si hay colisión, esperar
P-Persistente:
• Transmitir tan pronto como el canal esté libre con una probabilidad P
• En otro caso, esperar una unidad de tiempo y repetir el proceso
• Si hay colisión, esperar

Figura 16.1. Persistencia y espera en CSMA.

primero de ellos, denominado **CSMA no persistente**, una estación que desee transmitir escuchará el medio y procederá según las siguientes reglas:

1. Si el medio se encuentra libre, transmite; en otro caso se aplica el paso 2.
2. Si el medio se encuentra ocupado, espera una cierta cantidad de tiempo obtenida de una distribución de probabilidad (retardo de retransmisión) y repite el paso 1.

El uso de retardos aleatorios reduce la probabilidad de las colisiones. Para ver esto mejor, considérese que dos estaciones se encuentran listas para transmitir aproximadamente al mismo tiempo, mientras que otra transmisión se encuentra en curso. Si ambas estaciones esperan la misma cantidad de tiempo antes de intentarlo de nuevo, las dos intentarán transmitir aproximadamente al mismo tiempo. Un problema de CSMA no persistente es que se desaprovecha la capacidad debido a que el medio permanecerá libre justo tras el fin de una transmisión incluso si una o más estaciones se encuentran listas para transmitir.

Para evitar los intervalos en los que el medio se encuentra libre se puede utilizar el protocolo **CSMA 1-persistente**. Una estación que desee transmitir escuchará el medio y actuará de acuerdo con las siguientes reglas:

1. Si el medio se encuentra libre, transmite; en otro caso se aplica el paso 2.
2. Si el medio está ocupado, continúa escuchando hasta que el canal se detecte libre, momento en el cual se transmite inmediatamente.

Mientras que con CSMA no persistente una estación actúa de un modo más deferente, en el caso de CSMA 1-persistente el comportamiento es más egoísta. Si dos o más estaciones desean transmitir, se garantiza que se producirá una colisión. La técnica sólo toma medidas tras la colisión.

La técnica **CSMA *p*-persistente** representa un compromiso entre reducir el número de colisiones, como en el caso de no persistente, y reducir el tiempo de desocupación del canal, como en 1-persistente. Las reglas que se aplican son las siguientes:

1. Si el medio se encuentra libre, entonces se transmite con una probabilidad p y se espera una unidad de tiempo con una probabilidad $(1 - p)$. La unidad de tiempo es generalmente igual al retardo máximo de propagación.

2. Si el medio está ocupado, se continúa escuchando hasta que se detecte libre y se repite el paso 1.
3. Si la transmisión se ha retardado una unidad de tiempo, se repite el paso 1.

La cuestión que se plantea es la de cuál es un valor efectivo para p. El principal problema que se debe evitar es el de la inestabilidad en condiciones de carga elevada. Considérese el caso en el que n estaciones disponen de tramas para enviar mientras que se está produciendo una transmisión. Cuando ésta termine, el número esperado de estaciones que intentarán transmitir es igual a n veces la probabilidad de transmitir, siendo n el número de estaciones que se encuentran listas para transmitir; esto es, np. Si np es mayor que 1, existirán, en término medio, varias estaciones que intentarán transmitir y se producirá una colisión. Lo que es más, tan pronto como estas estaciones se percaten de que su transmisión ha sufrido una colisión, volverán a intentarlo, casi garantizando así más colisiones. Otro hecho que agrava esta situación es que todos estos reintentos deberán competir con nuevas transmisiones realizadas por otras estaciones, lo que incrementa aún más la probabilidad de colisión. Eventualmente, todas las estaciones estarán intentando enviar, causando colisiones de forma continua y haciendo así que el rendimiento decaiga hasta cero. Para evitar esta catástrofe, np debe ser menor que 1 para los picos esperados de n. Por tanto, si es de esperar que las condiciones de alta carga se den con cierta regularidad, p debe ser pequeño. Sin embargo, a medida que p se hace pequeño, las estaciones esperarán más tiempo hasta intentar transmitir de nuevo. En condiciones de baja carga esto conducirá a retardos muy elevados. Por ejemplo, si sólo una estación desease transmitir, el número esperado de iteraciones del paso 1 es de $1/p$ (*véase* el Ejercicio 16.2). Así, para $p = 0{,}1$ y en condiciones de baja carga, una estación esperará una media de 9 unidades de tiempo antes de transmitir sobre un medio libre.

Descripción de CSMA/CD

CSMA, aunque más eficiente que ALOHA y que ALOHA ranurado, presenta también una ineficiencia manifiesta. Cuando dos tramas colisionan, el medio permanece inutilizable mientras dure la transmisión de ambas tramas dañadas. En el caso de que la longitud de las tramas sea elevada en comparación con el tiempo de propagación, la cantidad de tiempo desaprovechado puede ser considerable. Este desaprovechamiento de la capacidad puede reducirse si una estación continúa escuchando el medio mientras dure la transmisión. La inclusión de esta característica conduce a las siguientes reglas para CSMA/CD:

1. Si el medio se encuentra libre, transmite; en otro caso se aplica el paso 2.
2. Si el medio se encuentra ocupado, continúa escuchando hasta que el canal se libere, en cuyo caso transmite inmediatamente.
3. Si se detecta una colisión durante la transmisión, se transmite una pequeña señal de interferencia para asegurarse de que todas las estaciones constaten la colisión. A continuación, se deja de transmitir.
4. Tras la emisión de la señal de interferencia, la estación espera una cantidad aleatoria de tiempo conocida como **espera** (*backoff*), intentando transmitir de nuevo a continuación (volviendo al paso 1).

La Figura 16.2 ilustra esta técnica para un bus en banda base. En t_0, la estación A comienza a transmitir un paquete destinado a D. En t_1, tanto B como C están listos para transmitir. B detecta una transmisión en curso y pospone la suya. C, sin embargo, aún no se ha percatado de la transmisión de A (porque el primer bit de la transmisión de A todavía no ha alcanzado el punto en el que se encuentra C) y comienza a transmitir. Cuando la transmisión de A alcanza C en t_2, C detecta la

colisión y cesa de transmitir. El efecto de la colisión se propaga hasta A, punto en el que es detectado en un instante posterior, t_3, siendo en ese momento cuando A deja de transmitir.

Con CSMA/CD, la cantidad de tiempo desaprovechado se reduce al tiempo que se necesita para detectar una colisión. La pregunta es, por supuesto, cuánto tiempo lleva esto. Consideremos el caso de un bus en banda base y dos estaciones tan separadas como sea posible. Por ejemplo, en la Figura 16.2, supongamos que la estación A comienza a transmitir y que, justo antes de que la transmisión alcance a D, éste se encuentra listo para transmitir. Puesto que D no es todavía consciente de la transmisión de A, aquél comenzará a transmitir. La colisión se producirá casi inmediatamente y así será reconocida por D. Sin embargo, la colisión deberá propagarse por todo el medio hasta alcanzar a A antes de que éste se percate. Siguiendo este razonamiento podemos concluir que la cantidad de tiempo involucrada en detectar una colisión no es mayor que dos veces el retardo de propagación extremo a extremo.

Una regla importante aplicada en la mayor parte de los sistemas CSMA/CD, incluyendo las normalizaciones IEEE, consiste en que la trama debe ser lo suficientemente larga como para permitir la detección de la colisión antes de que finalice la transmisión. Si se usan tramas más cortas,

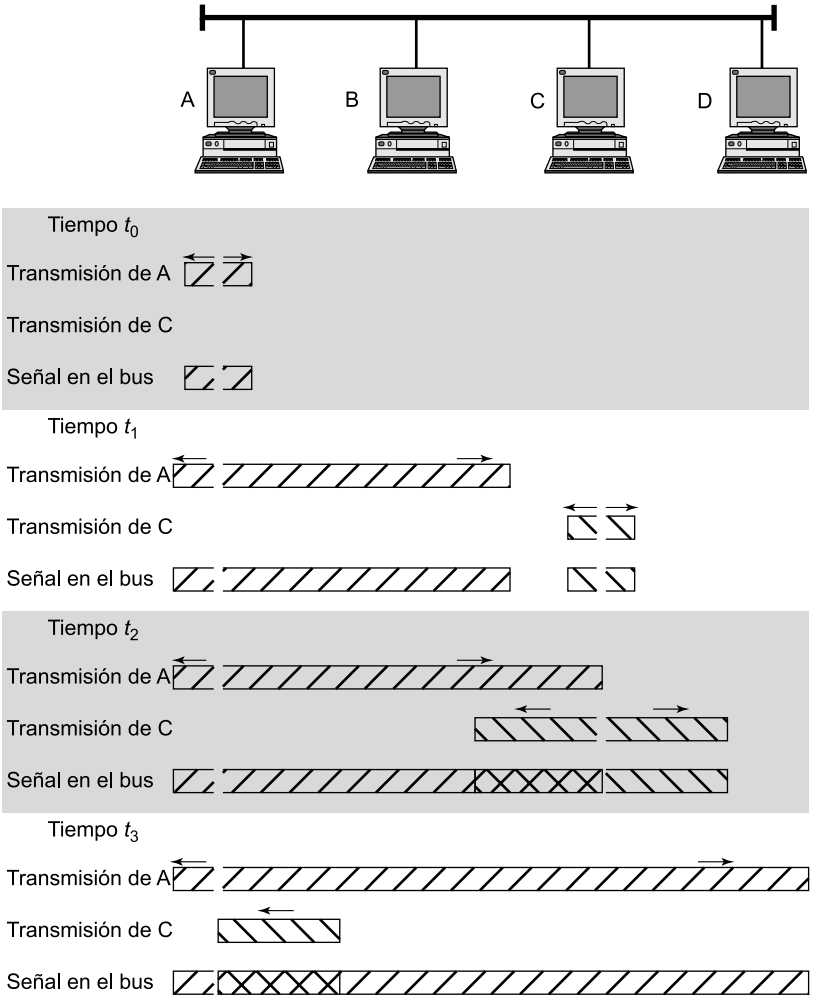


Figura 16.2. Funcionamiento de CSMA/CD.

no se produce la detección de la colisión, presentando la técnica CSMA/CD las mismas prestaciones que el protocolo CSMA menos eficiente.

En una red LAN CSMA/CD se plantea la cuestión de qué algoritmo de persistencia utilizar. Podría parecer sorprendente el hecho de que el algoritmo usado en el estándar IEEE 802.3 es el 1-persistente. Recuérdese que tanto el no persistente como el *p*-persistente presentan problemas de rendimiento. En el caso del no persistente, la capacidad se desaprovecha porque el medio permanece generalmente desocupado tras el fin de una transmisión, incluso si hay estaciones esperando para transmitir. En el caso del algoritmo *p*-persistente, el parámetro *p* debe ser lo suficientemente bajo como para evitar la inestabilidad, resultando ocasionalmente en retardos enormes en condiciones de carga elevada. El algoritmo 1-persistente, que implica, después de todo, hacer $p = 1$, parece ser incluso más inestable que el *p*-persistente debido a la avaricia de las estaciones. El punto a su favor es que el tiempo desaprovechado debido a las colisiones es muy pequeño (si las tramas son largas en comparación al retardo de propagación) y, considerando un tiempo de espera aleatorio, no es probable que las dos estaciones involucradas en una colisión vuelvan a estarlo en sus siguientes reintentos. Con objeto de asegurar que la espera mantenga la estabilidad, las redes IEEE 802.3 y Ethernet usan una técnica conocida como **espera exponencial binaria** (*binary exponential backoff*). En esta técnica, la estación intentará transmitir cada vez que colisione. Durante los primeros 10 intentos de retransmisión, el valor medio del tiempo de espera se dobla cada vez. A partir de ahí, este valor permanece igual durante 6 intentos adicionales. Después de 16 intentos sin éxito, la estación abandona e informa de un error. De esta forma, a medida que la congestión crece, las estaciones esperan para transmitir periodos de tiempo cada vez más largos, reduciendo así la probabilidad de una colisión.

La elegancia del algoritmo 1-persistente con espera exponencial binaria viene dada por su eficiencia frente a un amplio rango de condiciones de carga. En condiciones de baja carga, garantiza que una estación puede usar el canal tan pronto como éste se libere, en contraposición a los esquemas de no persistencia y *p*-persistencia. En condiciones de alta carga es, al menos, tan estable como las otras técnicas. No obstante, un desafortunado efecto del algoritmo de espera es que provoca un efecto de último-en-llegar, primero-en-salir: las estaciones sin colisiones o con muy pocas tendrán una oportunidad de transmitir antes de aquellas que llevan esperando más tiempo.

En buses en banda base, una colisión implicará la aparición de niveles de tensión superiores a los que cabría esperar en el caso de una transmisión sin colisiones. Consecuentemente, el estándar IEEE dicta que el transmisor detectará una colisión si la señal presente en el cable en el punto de conexión es mayor que el máximo nivel que se podría producir si se tratara de una única transmisión. Debido a que la señal se atenúa con la distancia, aparece un problema potencial: si dos estaciones muy distantes están transmitiendo, la señal que reciban la una de la otra estará muy atenuada. La energía de la señal recibida podría ser tan pequeña que, una vez sumada a la señal transmitida en el punto de conexión, pudiera ocurrir que la señal combinada no superara el umbral de continua (DC) preestablecido. Esta razón, entre otras, es la que ha justificado que el estándar de IEEE restrinja la longitud máxima del cable coaxial a 500 m en el 10BASE5 y a 200 m en el 10BASE2.

En la topología en estrella con pares trenzados (*véase* Figura 15.12) es posible utilizar un esquema de detección de colisiones mucho más sencillo. En este caso, la detección de colisiones se basa en magnitudes lógicas en lugar de utilizar niveles de tensión. Se determina que hay colisión si en cualquiera de los concentradores (*hubs*) hay actividad (señal) en más de una entrada, generándose en este caso una señal especial denominada señal de presencia de colisión. Esta señal se genera y se envía mientras se detecte actividad en cualquiera de las líneas de entrada y es interpretada por todos los nodos como la ocurrencia de una colisión.

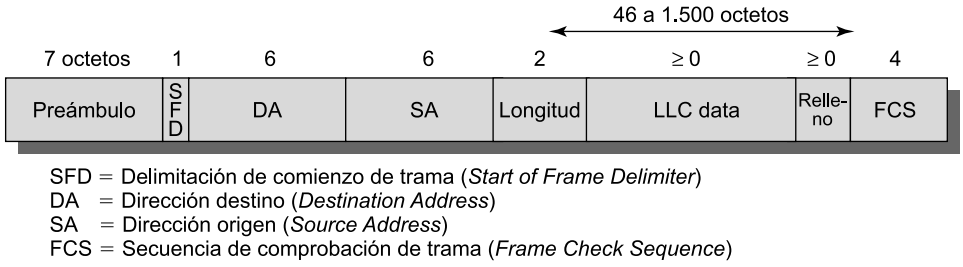


Figura 16.3. Formato de la trama IEEE 802.3.

Trama MAC

La Figura 16.3 muestra el formato de la trama del protocolo 802.3. Ésta consta de los siguientes campos:

- **Preámbulo:** el receptor usa 7 octetos de bits ceros y unos alternados para establecer la sincronización entre el emisor y el receptor.
- **Delimitador del comienzo de la trama (SFD, *Start Frame Delimiter*):** consiste en la secuencia de bits 10101011, que indica el comienzo real de la trama y posibilita que el receptor pueda localizar el primer bit del resto de la trama.
- **Dirección de destino (DA, *Destination Address*):** especifica la estación o estaciones a las que va dirigida la trama. Puede tratarse de una única dirección física, una dirección de grupo o una dirección global.
- **Dirección de origen (SA, *Source Address*):** especifica la estación que envió la trama.
- **Longitud/Tipo:** contiene la longitud del campo de datos LLC expresado en octetos, o el campo Tipo de Ethernet, dependiendo de que la trama siga la norma IEEE 802.3 o la especificación primitiva de Ethernet. En cualquier caso, el tamaño máximo de la trama, excluyendo el preámbulo y el SFD, es de 1518 octetos.
- **Datos LLC:** unidad de datos proporcionada por el LLC.
- **Relleno:** octetos añadidos para asegurar que la trama sea lo suficientemente larga como para que la técnica de detección de colisiones (CD) funcione correctamente.
- **Secuencia de Comprobación de Trama (FCS, *Frame Check Sequence*):** comprobación de redundancia cíclica de 32 bits, calculada teniendo en cuenta todos los campos excepto el preámbulo, el SFD y el FCS.

ESPECIFICACIONES IEEE 802.3 10 Mbps (ETHERNET)

El comité IEEE 802.3 ha sido el más activo en la definición de distintas configuraciones físicas alternativas. Esta proliferación tiene sus ventajas e inconvenientes. Lo positivo es que la normalización responde a la evolución de la tecnología, mientras que el aspecto negativo es que el consumidor, por no mencionar al potencial proveedor, se encuentra con una gran variedad de opciones. Sin embargo, el comité ha trabajado mucho para asegurar que las distintas opciones puedan ser integradas fácilmente en una configuración que satisfaga un gran número de necesidades. Así, el usuario que tiene un conjunto complejo de requisitos puede encontrar una ventaja en la flexibilidad y en la variedad del estándar 802.3.

El comité ha desarrollado una notación concisa con el fin de distinguir las diferentes implementaciones disponibles:

⟨velocidad de transmisión en Mbps⟩⟨método de señalización⟩
longitud máxima del segmento en centenas de metros⟩

Las alternativas definidas son[1]:

- **10BASE5:** especifica el uso de cable coaxial de 50 ohmios y señalización digital Manchester[2]. La longitud máxima del segmento de cable se fija a 500 metros. Esta longitud se puede extender mediante la utilización de repetidores. Un repetidor es transparente al nivel MAC y, dado que no gestiona memoria temporal, no aísla un segmento de otro. Así, por ejemplo, si dos estaciones en diferentes segmentos intentan transmitir al mismo tiempo, sus transmisiones colisionarán. Para evitar la aparición de bucles sólo se permite un único camino formado por segmentos y repetidores entre cualesquiera dos estaciones. La normalización permite un máximo de cuatro repetidores en el camino entre cualesquiera dos estaciones, ampliándose así la longitud efectiva del medio hasta 2,5 km.
- **10BASE2:** es similar a 10BASE5, excepto por el uso de un cable más fino que admite tomas de conexión para distancias más cortas que el cable de 10BASE5. Se trata de una alternativa menos costosa a aquél.
- **10BASE-T:** utiliza par trenzado no apantallado en una topología en estrella. Dada la alta velocidad y la baja calidad de las transmisiones sobre este tipo de cable, la longitud de cada enlace se restringe a 100 m. Como alternativa se puede utilizar un enlace de fibra óptica, en cuyo caso la longitud máxima es de 500 m.
- **10BASE-F:** contiene tres especificaciones: una topología en estrella pasiva para la interconexión de estaciones y repetidores con segmentos de hasta 1 km de longitud; un enlace punto a punto que puede ser usado para conectar estaciones o repetidores separados hasta 2 km; y un enlace punto a punto que puede usarse para conectar repetidores a una distancia máxima de 2 km.

Obsérvese que 10BASE-T y 10BASE-F no siguen la notación: «T» se usa para par trenzado y «F» para fibra óptica. La Tabla 16.2 resume estas opciones. Todas las alternativas enumeradas en la tabla especifican una velocidad de datos de 10 Mbps. Además de estas alternativas, existen varias versiones que funcionan a 100 Mbps, 1 Gbps y 10 Gbps, que serán estudiadas más adelante en esta sección.

ESPECIFICACIONES IEEE 802.3 100 Mbps (FAST ETHERNET)

Fast Ethernet es un conjunto de especificaciones desarrolladas por el comité IEEE 802.3 con el fin de proporcionar una red LAN de bajo coste compatible con Ethernet que funcione a 100 Mbps. La designación genérica para estos estándares es 100BASE-T. El comité definió varias alternativas para diferentes medios de transmisión.

[1] Existe también la opción 1BASE-T, que define un sistema de par trenzado a 1 Mbps usando una topología en estrella. Esta opción está obsoleta. Está también la opción 10BROAD36, que corresponde a un bus en banda ancha y que se usa muy poco.

[2] *Véase* Sección 5.1.

Tabla 16.2. Alternativas para el medio de transmisión en la capa física IEEE 802.3 a 10 Mbps.

	10BASE5	10BASE2	10BASE-T	10BASE-FP
Medio de transmisión	Cable coaxial (50 ohm)	Cable coaxial (50 ohm)	Par trenzado no apantallado	Par de fibra óptica a 850 nm
Técnica de señalización	Banda base (Manchester)	Banda base (Manchester)	Banda base (Manchester)	Manchester/ on-off
Topología	Bus	Bus	Estrella	Estrella
Longitud máxima del segmento (m)	500	185	100	500
Nodos por segmento	100	30	—	33
Diámetro del cable (mm)	10	5	0,4 a 0,6	62,5/125 μm

La Figura 16.4 muestra la terminología utilizada en las distintas especificaciones e indica, asimismo, el medio usado. Todas las opciones 100BASE-T usan el protocolo MAC y el formato de la trama IEEE 802.3. 100BASE-X identifica al conjunto de opciones que usan las especificaciones del medio físico definidas originalmente para FDDI (*Fiber Distributed Data Interface*). Todos los esquemas 100BASE-X emplean dos enlaces físicos entre los nodos, uno para transmisión y otro para recepción. 100BASE-X hace uso de pares trenzado apantallados (STP) o pares trenzados no apantallados (UTP) de alta calidad (categoría 5), mientras que 100BASE-FX hace uso de fibra óptica.

En muchos edificios, cualquiera de las opciones 100BASE-X requiere la instalación de nuevo cableado. En estos casos, 100BASE-T4 define una alternativa menos costosa que puede utilizar UTP de voz de categoría 3 además de UTP de categoría 5 de alta calidad[3]. Para alcanzar los 100 Mbps en cables de baja calidad, 100BASE-T4 especifica el uso de 4 líneas de par trenzado entre los nodos, de los cuales tres se usan simultáneamente para la transmisión de datos en una dirección.

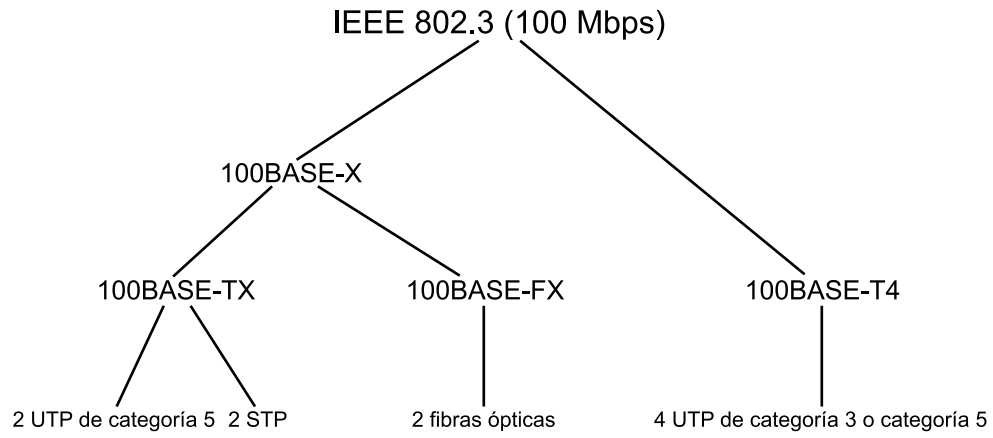


Figura 16.4. Opciones 100BASE-T en IEEE 802.3.

[3] *Véase* el Capítulo 4 para un estudio del cable de tipo 3 y tipo 5.

La topología de todas las opciones 100BASE-T es similar a la de 10BASE-T, que corresponde a una estrella.

La Tabla 16.3 resume las características más importantes de las opciones 100BASE-T.

Tabla 16.3. Alternativas para el medio de transmisión en la capa física IEEE 802.3 100BASE-T.

	100BASE-TX		100BASE-FX	100BASE-T4
Medio de transmisión	2 pares, STP	2 pares, UTP categoría 5	2 fibras ópticas	4 pares, UTP categoría 3, 4 o 5
Técnica de señalización	MLT-3	MLT-3	4B5B, NRZI	8B6T, NRZ
Velocidad de transmisión	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Longitud máxima del segmento	100 m	100 m	100 m	100 m
Cobertura de la red	200 m	200 m	400 m	200 m

100BASE-X

En todos los medios de transmisión especificados en 100BASE-X, los 100 Mbps se consiguen en un solo sentido utilizando un único enlace (par trenzado individual, fibra óptica individual). Para tal fin, en todos los medios se necesita un esquema de codificación de señal que sea efectivo y eficiente. El esquema elegido se definió originalmente para FDDI y se denomina 4B/5B-NRZI. Este esquema se modifica y particulariza en cada opción. *Véase* el Apéndice 16A para un estudio del mismo.

El esquema 100BASE-X incluye dos especificaciones para el medio físico, una para par trenzado, conocida como 100BASE-TX, y otra para fibra óptica, denominada 100BASE-FX.

100BASE-TX utiliza dos pares de cable de par trenzado, uno para transmisión y otro para recepción. Se permiten tanto STP como UTP de categoría 5, y se usa el esquema de señalización MLT-3 (descrito en el Apéndice 16A).

100BASE-FX utiliza dos fibras ópticas, una para transmitir y otra para recibir. En 100BASE-FX es necesario el uso de algún método para convertir la secuencia de grupos de código 4B/5B-NRZI en señales ópticas. Esta conversión se denomina modulación en intensidad. Un uno binario se representa por un haz o pulso de luz, mientras que un cero binario se representa por la ausencia de pulso de luz o por uno de muy baja intensidad.

100BASE-T4

100BASE-T4 está pensado para ofrecer una velocidad de transmisión de datos de 100 Mbps a través de cable de tipo 3 de baja calidad, siguiendo la idea de poder reutilizar las instalaciones existentes de este tipo de cable en edificios de oficinas. La especificación también permite el uso opcional de cable de tipo 5. 100BASE-T4 no transmite una señal continua entre paquetes, lo que lo hace útil para sistemas alimentados por baterías.

En 100BASE-T4, al utilizar cable de tipo 3 para voz, no es de esperar que los 100 Mbps se obtengan utilizando un único par trenzado. Por el contrario, 100BASE-T4 especifica que la secuencia de datos a transmitir se divida en tres secuencias distintas, cada una de las cuales se transmitirá a una velocidad de transmisión efectiva de 33,3 Mbps. Se usan cuatro pares trenzados, de modo que los datos se transmiten haciendo uso de tres pares y se reciben a través de otros tres. Por tanto, dos de los pares deben configurarse para una transmisión bidireccional.

Como en el caso de 100BASE-X, en 100BASE-T4 no se emplea un esquema de codificación NRZ. Esto requeriría una velocidad de transmisión de datos de 33 Mbps a través de cada par trenzado y no proporcionaría sincronización. En su lugar, se usa un esquema de señalización ternario conocido como 8B6T (descrito en el Apéndice 16A).

Funcionamiento *full-duplex*

Una red Ethernet tradicional es *semi-duplex*: una estación puede transmitir una trama o recibirla, pero no ambas cosas simultáneamente. En el modo de funcionamiento *full-duplex*, una estación puede transmitir y recibir al mismo tiempo, de manera que una Ethernet a 100 Mbps en *full-duplex* alcanzaría, teóricamente, una velocidad de 200 Mbps.

Es preciso introducir algunos cambios para funcionar en modo *full-duplex*. Las estaciones conectadas deben tener tarjetas adaptadoras *full-duplex* en lugar de las *semi-duplex* tradicionales. El punto central en la topología en estrella no puede ser simplemente un repetidor multipuesto, sino un concentrador conmutado. En este caso, cada estación constituye un dominio de colisión separado. De hecho, las colisiones no se producen y el algoritmo CSMA/CD no es necesario. Se sigue utilizando, sin embargo, el mismo formato de trama MAC 802.3 y las estaciones pueden continuar ejecutando el algoritmo CSMA/CD a pesar de que jamás se detectará una colisión.

Configuraciones mixtas

Uno de los aspectos positivos de Fast Ethernet es que soporta cómodamente una configuración que incluya diferentes redes LAN a 10 Mbps así como las nuevas a 100 Mbps. Por ejemplo, la tecnología a 100 Mbps puede ser usada como una red LAN troncal que interconecte un cierto número de concentradores de 10 Mbps. Muchas estaciones pueden conectarse a estos concentradores de 10 Mbps usando el estándar 10BASE-T. Los concentradores se conectan a otros concentradores conmutados del tipo 100BASE-T y que soporten enlaces de 10 y 100 Mbps. El resto de estaciones de alta capacidad y servidores pueden conectarse directamente a estos conmutadores 10/100, los cuales se conectan a concentradores de 100 Mbps usando enlaces de 100 Mbps. Los concentradores de 100 Mbps proporcionan una red troncal que puede ser conectada a una red WAN exterior a través de un encaminador.

GIGABIT ETHERNET

A finales del año 1995, el comité IEEE 802.3 formó el grupo de trabajo de alta velocidad con el fin de investigar estrategias para transmitir paquetes con formato Ethernet a velocidades del orden de Gigabits por segundo. Desde entonces se han especificado un conjunto de estándares a 1.000 Mbps.

La estrategia seguida en Gigabit Ethernet es la misma que la adoptada en Fast Ethernet. A pesar de que se define un nuevo medio y una especificación para la transmisión, se sigue adoptando

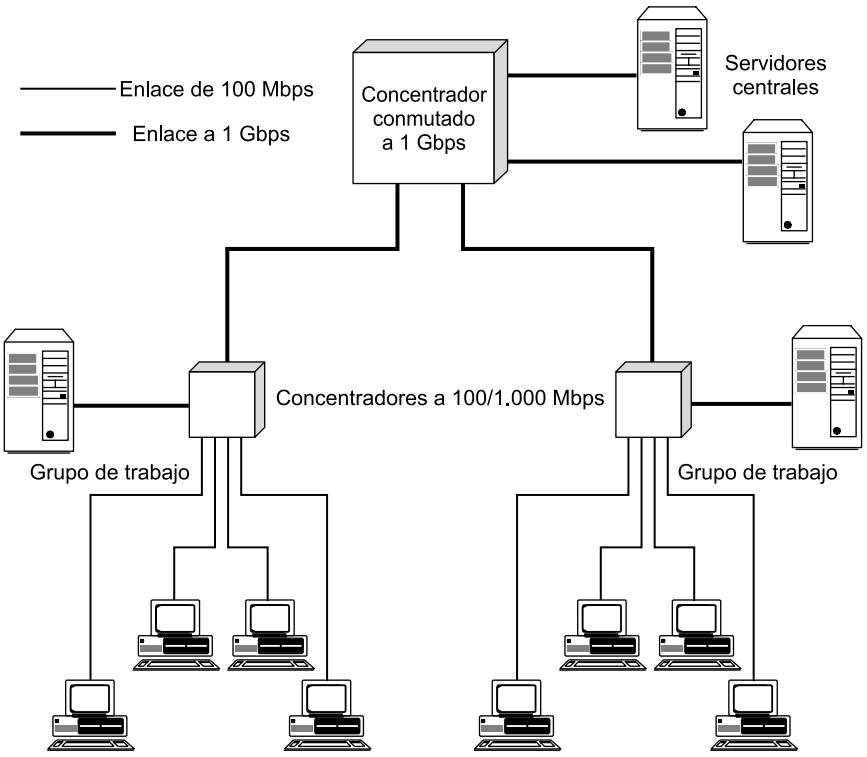


Figura 16.5. Ejemplo de configuración para Gigabit Ethernet.

tanto el protocolo CSMA/CD como el formato de trama de sus predecesores Ethernet a 10 Mbps y 100 Mbps. Es compatible con 100BASE-T y 10BASE-T, facilitando la migración. La demanda de tecnología Gigabit Ethernet ha crecido debido a que las organizaciones están adoptando cada vez más 100BASE-T, lo que implica cantidades enormes de tráfico en las líneas troncales.

En la Figura 16.5 se muestra una aplicación típica de Gigabit Ethernet. Un conmutador a 1 Gbps proporciona la conectividad entre los servidores centrales y entre los concentradores de alta velocidad. Cada concentrador se conecta a la línea troncal mediante un enlace a 1 Gbps y conecta, además, a los servidores de cada concentrador, a la vez que ofrece enlaces a 100 Mbps para conectar a estaciones de trabajo, servidores y otros concentradores a 100 Mbps.

Capa de acceso al medio

La especificación a 1.000 Mbps utiliza el mismo formato para las tramas y protocolos que el CSMA/CD usado en las versiones de IEEE 802.3 a 10 Mbps y 100 Mbps. Se han introducido dos mejoras respecto al esquema CSMA/CD básico en lo que se refiere al funcionamiento de los concentradores (*véase* Figura 15.13b):

- **Extensión de la portadora:** esta mejora consiste en añadir una serie de símbolos al final de una trama MAC corta, de tal manera que el bloque resultante tenga una duración equivalente a 4.096 bits, mucho mayor que los 512 exigidos en el estándar a 10 y 100 Mbps. El objetivo es que la longitud de la trama, es decir, el tiempo de transmisión, sea mayor que el tiempo de propagación a 1 Gbps.

- **Ráfagas de tramas:** esta funcionalidad permite que se transmitan de forma consecutiva varias tramas cortas (sin superar un límite) sin necesidad de dejar el control del CSMA/CD. Las ráfagas de tramas evitan la redundancia y gasto que conlleva la técnica de la extensión de la portadora, en el caso de que una estación tenga preparadas para transmitir varias tramas pequeñas.

En el conmutador (*véase* Figura 15.13c), que facilita un acceso al medio dedicado, no son necesarias las técnicas de extensión de la portadora ni la de ráfagas de tramas. Esto se debe a que una estación puede transmitir y recibir simultáneamente sin interferencias y sin necesidad de competir para acceder al medio compartido.

Capa física

La especificación actual de IEEE 802.3 a 1 Gbps define las siguientes alternativas (*véase* Figura 16.6):

- **1000BASE-SX:** esta opción, en la que se usan longitudes de onda pequeñas, proporciona enlaces dúplex de 275 m usando fibras multimodo de 62,5 μm o hasta 550 m con fibras multimodo de 50 μm. Las longitudes de onda están en el intervalo comprendido entre 770 y 860 nm.
- **1000BASE-LX:** esta alternativa, en la que se utilizan longitudes de onda mayores, proporciona enlaces dúplex de 550 m con fibras multimodo de 62,5 μm o 50 μm, o de 5 km con fibras monomodo de 10 μm. Las longitudes de onda están entre los 1.270 y los 1.355 nm.
- **1000BASE-CX:** esta opción proporciona enlaces de 1 Gbps entre dispositivos localizados dentro de una habitación (o armario de conexiones) utilizando latiguillos de cobre (cables de pares trenzados de menos de 25 m con un apantallamiento especial). Cada enlace consiste en dos pares trenzados apantallados, cada uno de los cuales se usa en un sentido.
- **1000BASE-T:** esta opción utiliza cuatro pares no apantallados tipo 5 para conectar dispositivos separados hasta 1.000 m.

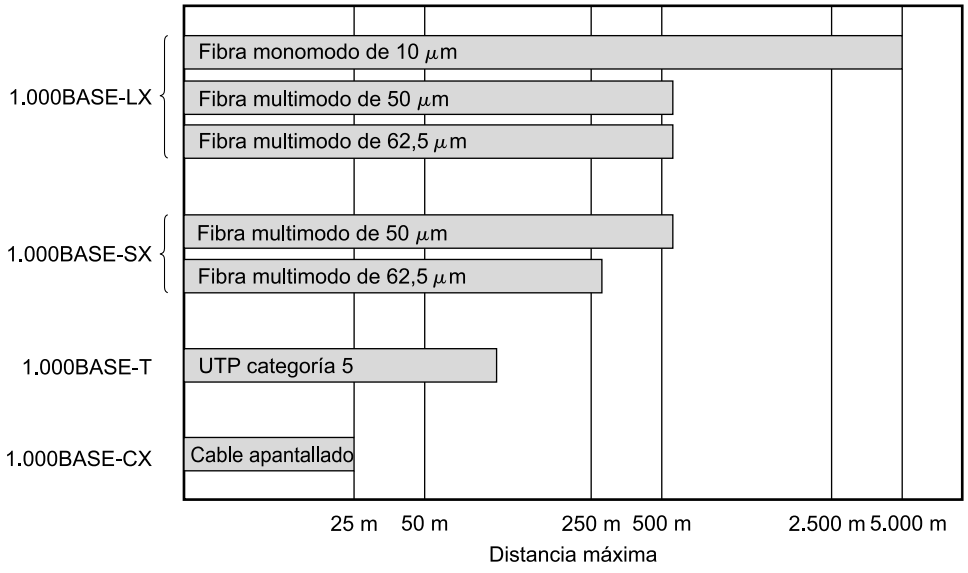


Figura 16.6. Opciones del medio en Gigabit Ethernet (escala logarítmica).

El esquema de codificación de señal que se usa para las tres primeras opciones de Gigabit Ethernet es 8B/10B, descrito en el Apéndice 16A. En el caso de 1000BASE-T se usa 4D-PAM5, una técnica relativamente complicada cuya descripción queda fuera de este contexto.

ETHERNET DE 10 Gbps

Con los productos gigabit todavía bastante nuevos, la atención se ha desplazado en los últimos años hacia Ethernet con capacidad de 10 Gbps. El principal requisito que ha motivado este interés ha sido el incremento en el tráfico de Internet e intranets. Este incremento espectacular se ha debido a una serie de factores:

- Incremento en el número de conexiones de red.
- Incremento en la velocidad de conexión de cada estación final (por ejemplo, usuarios de 10 Mbps migrando hacia 100 Mbps, usuarios de líneas analógicas de 56 kbps migrando hacia soluciones DSL y módem de cable).
- Incremento en el despliegue de aplicaciones demandantes de ancho de banda, como el vídeo de alta calidad.
- Incremento en el hospedaje de web y el tráfico de las aplicaciones de hospedaje.

En principio, los administradores de red podrán usar Ethernet de 10 Gbps para construir redes troncales locales de alta velocidad que proporcionarán interconexión a conmutadores de alta capacidad. A medida que la demanda de ancho de banda crezca, Ethernet de 10 Gbps podrá ser desplegada a lo largo de toda la red, interconectando agrupaciones centralizadas de servidores, redes troncales y proporcionando cobertura para toda un área. Esta tecnología permite que los proveedores de servicios de Internet (ISP, *Internet Service Providers*) y los proveedores de servicios de red (NSP, *Network Service Providers*) puedan ofrecer enlaces de alta velocidad a un costo reducido entre encaminadores y conmutadores adyacentes.

Esta tecnología permite también la construcción de redes de área metropolitana (MAN, *Metropolitan Area Network*) y de área amplia (WAN, *Wide Area Network*) que conecten redes LAN geográficamente dispersas entre distintos puntos de presencia. Ethernet comienza así a competir con ATM y otras tecnologías de transmisión de área amplia. En la mayoría de los casos en los que los requisitos del cliente son el transporte de datos y de TCP/IP, Ethernet a 10 Gbps proporciona un valor añadido sustancial sobre el transporte ofrecido por ATM, tanto para los usuarios finales de la red como para los proveedores del servicio:

- No se requiere una conversión costosa y demandante de ancho de banda entre paquetes Ethernet y celdas ATM. La red es Ethernet extremo a extremo.
- La combinación de IP y Ethernet ofrece calidad de servicio y capacidades para establecer políticas de tráfico que se aproximan a las que brinda ATM, de manera que tanto usuarios como proveedores tienen a su disposición una tecnología de ingeniería de tráfico avanzada.
- Ethernet de 10 Gigabits recoge un amplio abanico de interfaces ópticas estándares (longitudes de onda y distancias), optimizando tanto su funcionamiento como su coste para aplicaciones LAN, MAN o WAN.

Las distancias máximas de los enlaces cubren un intervalo de aplicaciones, desde 300 m hasta 40 km. Los enlaces funcionan exclusivamente en modo *full-duplex*, usando diversos medios físicos de fibra óptica.

Han sido definidas cuatro opciones para la capa física en Ethernet de 10 Gbps (*véase* la Figura 16.7):

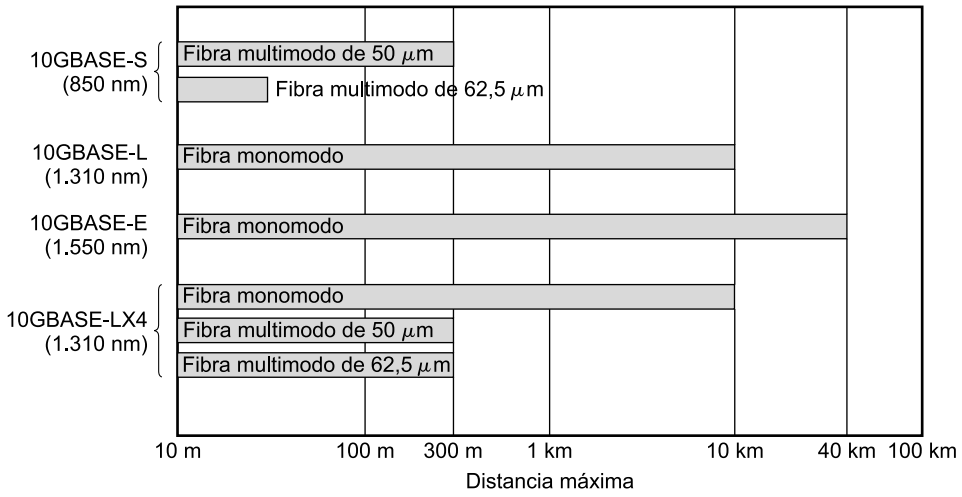


Figura 16.7. Velocidad y opciones de distancia en Ethernet a 10 Gbps (escala logarítmica).

- **10GBASE-S (corta):** diseñada para transmisiones de 850 nm sobre fibras multimodo. Este medio puede alcanzar distancias de hasta 300 m.
- **10GBASE-L (larga):** diseñada para transmisiones de 1.310 nm sobre fibras monomodo. Puede alcanzar distancias de hasta 10 km.
- **10GBASE-E (extendida):** diseñada para transmisiones de 1.550 nm sobre fibras monomodo. Puede alcanzar distancias de hasta 40 km.
- **10GBASE-LX4:** diseñada para transmisiones de 1.310 nm sobre fibras monomodo o multimodo, alcanzándose distancias de hasta 10 km. Este medio utiliza multiplexación por división de longitud de onda (WDM, *Wavelength Division Multiplexing*) para multiplexar el flujo de bits sobre cuatro ondas de luz.

16.3. ANILLO CON PASO DE TESTIGO

El estándar IEEE 802.5 de anillo con paso de testigo (*token ring*) es una consecuencia de las redes LAN comerciales de paso de testigo de IBM. Dada la presencia de IBM en el mercado corporativo, las redes LAN de paso de testigo han ganado una amplia aceptación. No obstante, no han alcanzado nunca la popularidad de los sistemas tipo Ethernet. Pese a que actualmente existe una extensa base de productos de paso de testigo instalados, todo apunta a que este mercado declinará rápidamente en los próximos años.

Comenzaremos con una breve introducción al funcionamiento de una red LAN en anillo. Posteriormente abordaremos el estándar IEEE 802.5.

FUNCIONAMIENTO DEL ANILLO

Un anillo consta de varios repetidores, cada uno de ellos conectado a otros dos por líneas de transmisión unidireccionales y formando así un único camino cerrado. Los datos se transmiten secuencialmente, bit a bit, alrededor del anillo desde un repetidor hasta el siguiente. Cada repetidor regenera cada bit y lo retransmite.

Para que un anillo funcione como una red de comunicaciones son necesarias tres funciones que son llevadas a cabo por los repetidores: inserción de datos, recepción de datos y eliminación de datos. Cada repetidor, además de servir como elemento activo en el anillo, sirve como punto de conexión de cada dispositivo. Los datos son transmitidos en paquetes, conteniendo cada uno de ellos un campo de dirección de destino. El campo de dirección de un paquete, al circular por el anillo y atravesar un repetidor, es copiado por éste; si la dirección coincide con la de la estación, se copia el resto del paquete.

Los repetidores realizan las funciones de inserción y recepción de datos de forma análoga a como lo hacen las tomas que sirven como puntos de conexión de dispositivos en un bus o en un árbol. La eliminación de datos es, sin embargo, más complicada en el caso de un anillo. Las señales en un bus o en un árbol se insertan en la línea, se propagan hacia los extremos y son absorbidas por los terminadores; así, el bus o el árbol están libres de los datos poco después de haber cesado la comunicación. Sin embargo, dado que el anillo es un bucle cerrado, el paquete circulará indefinidamente a menos que sea eliminado. Un paquete puede ser eliminado por el repetidor destino. Otra alternativa consiste en que cada paquete sea eliminado por el repetidor que lo emitió después de que haya dado una vuelta completa en el anillo. Esta última aproximación es mejor debido a que (1) permite confirmaciones automáticas y (2) permite direccionamiento múltiple: un paquete puede ser enviado simultáneamente a varias estaciones.

Se puede hacer uso de una gran diversidad de estrategias para determinar cómo y cuándo insertar los paquetes en el anillo. Estas estrategias son, de hecho, protocolos de control de acceso al medio, siendo el más usual de ellos el anillo con paso de testigo.

Al repetidor, por tanto, se le pueden adjudicar dos funciones principales: (1) contribuir al funcionamiento adecuado del anillo dejando pasar todos los datos que lo atraviesan, y (2) ofrecer un punto de acceso a las estaciones conectadas para transmitir y recibir datos. Existen dos estados correspondientes a estos dos cometidos (*véase* Figura 16.8): estado de escucha y estado de transmisión.

En el estado de escucha cada bit recibido se retransmite con un pequeño retardo, necesario para permitir al repetidor realizar las funciones básicas. Idealmente, el retardo debe ser del orden del intervalo de duración de un bit (el tiempo que tarda el repetidor en transmitir un bit completo por la línea de salida). Estas funciones son:

- Búsqueda de secuencias de patrones de bits. Entre ellas está la dirección o direcciones de las estaciones conectadas. Otro patrón, usado en la estrategia de control con paso de testigo explicada más adelante, indica permiso para transmitir. Obsérvese que el repetidor debe tener conocimiento del formato de los paquetes para realizar la función de búsqueda.
- Copia de cada bit entrante y su envío a la estación conectada mientras se continúa con la retransmisión de cada bit. Esto se realizará para cada bit de cada paquete dirigido a la estación.

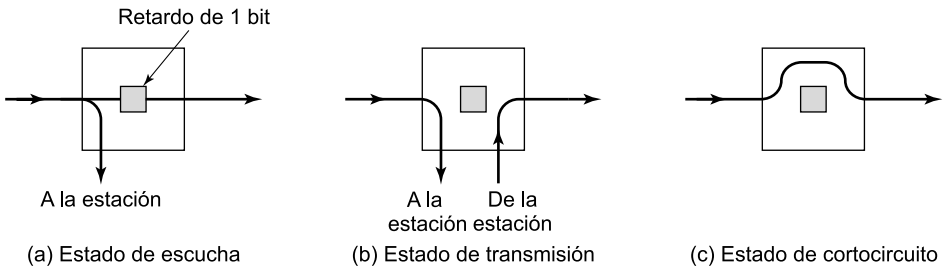


Figura 16.8. Estados del repetidor de un anillo.

- Modificación de un bit mientras circula. Los bits se pueden modificar en determinadas estrategias de control para, por ejemplo, indicar que el paquete ha sido copiado. Esto sirve como confirmación.

Cuando la estación dispone de datos a transmitir y el repetidor al que se encuentra conectada, de acuerdo con la estrategia de control, tiene permiso para hacerlo, este último entra en estado de transmisión. En este estado el repetidor recibe bits de la estación y los retransmite por la línea de salida. Durante el periodo de transmisión pueden aparecer bits por la línea de entrada del anillo. Existen dos posibles situaciones, tratadas de forma diferente:

- Los bits pueden proceder del mismo paquete que el repetidor está transmitiendo, lo cual sucederá si la «longitud de bit» del anillo es menor que el tamaño de paquete. En este caso, el repetidor pasa los bits hacia la estación, que puede comprobarlos como método de confirmación.
- En algunas estrategias de control se permite la existencia simultánea de más de un paquete en el anillo. Si el repetidor recibe bits de un paquete distinto al que está transmitiendo, debe almacenarlos temporalmente para retransmitirlos con posterioridad.

Estos dos estados, escucha y transmisión, son suficientes para un funcionamiento adecuado del anillo. Un tercer estado, estado de cortocircuito (*bypass*), resulta también útil. En este estado se puede activar un relé de cortocircuito, de manera que las señales propagadas atraviesan el repetidor sin más retardo que el de propagación en el medio. El relé de cortocircuito presenta dos ventajas: (1) proporciona una solución parcial al problema de fiabilidad discutido más adelante, y (2) mejora las prestaciones al eliminar los retardos del repetidor para aquellas estaciones del medio que no se encuentren activas.

CONTROL DE ACCESO AL MEDIO

La técnica de anillo con paso de testigo se basa en el uso de una trama pequeña, denominada testigo (*token*), que circula cuando todas las estaciones están libres. Cuando una estación desea transmitir debe esperar a que le llegue el testigo. En este caso, toma el testigo cambiando uno de sus bits, lo que lo convierte en la secuencia de comienzo de las tramas de datos. Posteriormente, la estación añade y transmite el resto de campos requeridos en la construcción de la trama.

Cuando una estación toma el testigo y comienza a transmitir, el testigo deja de estar presente en el anillo, de manera que el resto de estaciones que deseen transmitir deben esperar. La trama en el anillo realiza una vuelta completa y se absorbe en la estación transmisora, que insertará un nuevo testigo en el anillo cuando se cumplan las dos condiciones siguientes:

- La estación ha terminado la transmisión de su trama.
- Los bits iniciales de la trama transmitida hayan vuelto a la estación (después de una vuelta completa al anillo).

Si la longitud del anillo es menor que la longitud de la trama, la primera condición implica la segunda. En caso contrario, una estación podría liberar el testigo después de que haya terminado de transmitir, pero antes de que comience a recibir su propia transmisión. La segunda condición no es estrictamente necesaria, relajándose en la configuración conocida como liberación rápida del testigo (*early token release*). La ventaja que implica la imposición de la segunda condición es que asegura que, en un instante de tiempo dado, sólo puede haber una trama de datos en el medio y sólo puede estar transmitiendo una estación, simplificándose los procedimientos de recuperación de errores.

Una vez que se ha insertado un nuevo testigo en el anillo, la siguiente estación en la secuencia que disponga de datos a transmitir podrá tomar el testigo y llevar a cabo la transmisión. La Figura 16.9 ilustra la técnica. En el ejemplo, A envía una trama a C, que la recibe y, una vez que ha recibido también el testigo, envía sus propias tramas a A y D.

Obsérvese que en condiciones de baja carga, el anillo con paso de testigo presenta cierta ineficacia debido a que una estación debe esperar a recibir el testigo antes de transmitir. Sin embargo, en condiciones de carga elevada, que es la situación más preocupante, el anillo funciona como un sistema de turno rotatorio (*round-robin*), que es eficiente además de equitativo. Para ver esto, consideremos la configuración de la Figura 16.9. Después de que la estación A transmita, libera un testigo. La primera estación con opción de transmitir es D. Si lo hace, libera después un testigo y C es la siguiente que puede transmitir, y así sucesivamente.

La principal ventaja del anillo con paso de testigo es el control de acceso flexible que ofrece. En el esquema sencillo que se acaba de describir el acceso es equitativo. Es posible, además, utili-

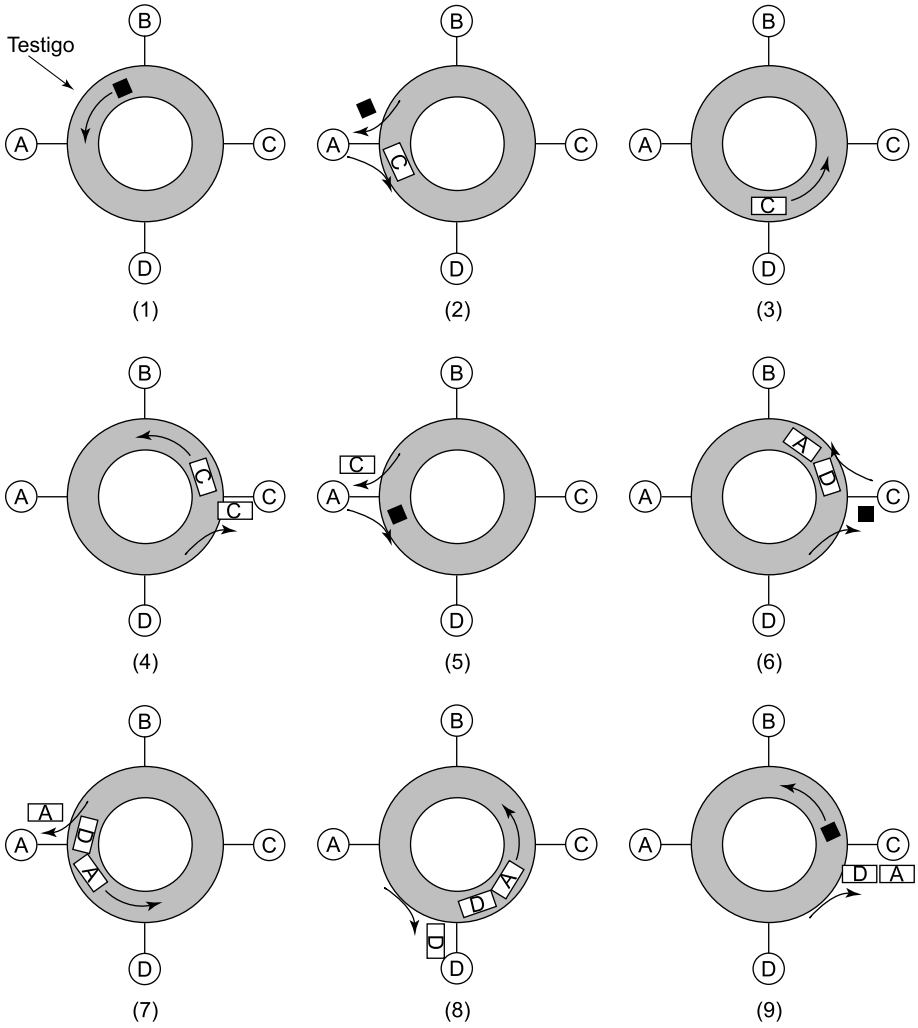


Figura 16.9. Funcionamiento del anillo con paso de testigo.

zar el anillo con paso de testigo para proporcionar prioridad y servicios con ancho de banda garantizado.

La principal desventaja del anillo con paso de testigo está en la necesidad de procedimientos para realizar el mantenimiento del anillo. La pérdida del testigo impide posteriores utilizaciones del anillo, mientras que una duplicidad del mismo puede interrumpir también el funcionamiento del anillo. Se puede seleccionar una estación como monitora para asegurar que haya únicamente un testigo en el anillo y para reinsertar un testigo libre en caso necesario.

La actualización de IEEE 802.5 de 1997 introdujo una nueva técnica de control de acceso al medio denominada **anillo con paso de testigo dedicado** (DTR, *Dedicated Token Ring*, haciendo uso de una topología en estrella. El algoritmo de paso de testigo se puede seguir utilizando en esta configuración, de manera que la capacidad del anillo siga siendo compartida puesto que el acceso al medio está determinado por el testigo. Sin embargo, es igualmente posible que el concentrador central funcione como un conmutador de la capa 2, de forma que la conexión entre cada estación y el conmutador funcione como un enlace punto a punto *full-duplex*. La especificación DTR define cómo utilizar las estaciones y concentradores en este modo conmutado. El concentrador DTR funciona como un retransmisor de tramas en lugar de ser un repetidor de bits. De esta manera, cada enlace desde el concentrador a las estaciones es un enlace dedicado con acceso inmediato, no usándose paso de testigo.

OPCIONES DE MEDIOS DE TRANSMISIÓN EN IEEE 802.5

El estándar 802.5 ofrece un amplio abanico de velocidades y medios de transmisión, como se muestra en la Tabla 16.4. El estándar fija un máximo para el tamaño de las tramas igual a 4.550 octetos a 4 Mbps y 18.200 octetos para 16 Mbps, 100 Mbps y 1 Gbps. Estos valores contrastan con los 1.518 octetos de las redes LAN IEEE 802.3. A 4 Mbps y a 16 Mbps se puede usar tanto el paso de testigo como la técnica DTR conmutada para el control de acceso al medio. A 100 Mbps, la utilización de la técnica DTR es obligatoria.

Tabla 16.4. Alternativas para el medio de transmisión en la capa física IEEE 802.5.

Velocidad de transmisión (Mbps)	4	16	100	100	1.000
Medio de transmisión	UTP, STP o fibra	UTP, STP o fibra	UTP o STP	Fibra	Fibra
Técnica de señalización	Manchester diferencial	Manchester diferencial	MLT-3	4B5B, NRZI	8B/10B
Tamaño máximo de la trama (octetos)	4.550	18.200	18.200	18.200	18.200
Control de acceso	TP o DTR	TP o DTR	DTR	DTR	DTR

UTP = par trenzado no apantallado (*unshielded twisted pair*).
STP = par trenzado apantallado (*shielded twisted pair*).
TP = control de acceso con paso de testigo (*token passing access control*).
DTR = anillo con paso de testigo dedicado (*dedicated token ring*).

El comité 802.5 completó el trabajo sobre la versión del anillo con paso de testigo a 1 Gbps en el año 2001, que, al igual que sucedió con la versión a 100 Mbps, adoptará la especificación de la capa física de 802.3.

16.4. CANAL DE FIBRA

A medida que han aumentado la velocidad y la capacidad de memoria de los computadores personales, estaciones de trabajo y servidores, y conforme las aplicaciones se han vuelto más complejas, con una mayor dependencia en gráficos y vídeo, la necesidad de mayor velocidad en el envío de datos a los procesadores ha aumentado. Este requisito afecta a dos métodos de comunicaciones de datos con el procesador: el canal de entrada/salida y las comunicaciones de red.

Un canal de entrada/salida es un enlace de comunicaciones directo punto a punto o multipunto, generalmente implementado en hardware y diseñado para conseguir altas velocidades de transmisión en distancias muy cortas. El canal de entrada/salida transfiere datos entre una memoria temporal en el dispositivo de origen y otra en el dispositivo de destino, limitándose únicamente a desplazar los contenidos del usuario desde un dispositivo al otro sin tener en cuenta el formato o significado de los datos. La lógica asociada al canal proporciona, generalmente, el control mínimo necesario para gestionar la transferencia, además de la detección de errores hardware. Los canales de entrada/salida manipulan por lo general transferencias entre procesadores y dispositivos periféricos, como discos, equipos gráficos, CD-ROM y dispositivos de entrada/salida de vídeo.

Una red es un conjunto de puntos de acceso interconectados con una estructura software de protocolos que posibilita la comunicación. La red admite generalmente diferentes tipos de transferencia de datos, haciendo uso del software para implementar los protocolos de red y para proporcionar control de flujo y detección y recuperación de errores. Como se ha discutido en este texto, las redes gestionan generalmente las transferencias entre sistemas finales en distancias locales, metropolitanas o de área amplia.

El canal de fibra está diseñado para combinar las características más sobresalientes de estas tecnologías —la sencillez y velocidad de las comunicaciones de canal con la flexibilidad e interconectividad que caracterizan a las comunicaciones de red basadas en protocolos—. Esta fusión de enfoques permite a los diseñadores de sistemas combinar la conexión tradicional de periféricos, la interconexión de redes estación-estación, la agrupación de procesadores débilmente acoplados y el uso de aplicaciones multimedia en una misma interfaz multiprotocolo. Entre los tipos de recursos orientados a canal que se incorporan en la arquitectura de protocolos del canal de fibra se encuentran:

- Modificadores de tipos de datos para encaminar la carga útil contenida en las tramas sobre memorias temporales de interfaz específicas.
- Elementos del nivel de enlace asociados con operaciones individuales de entrada/salida.
- Especificaciones de la interfaz de un protocolo para dar soporte a arquitecturas de canal de entrada/salida existentes, como la interfaz SCSI (*Small Computer System Interface*).

Entre los tipos de recursos orientados a red incorporados en la arquitectura de protocolos del canal de fibra se encuentran los siguientes:

- Multiplexación completa de tráfico entre múltiples destinos.
- Conectividad igual a igual (paritaria) entre cualquier par de puertos en una red de canal de fibra.
- Posibilidad de interconexión con otras tecnologías.

En función de las necesidades de la aplicación, tanto el enfoque de canal como el de red de comunicaciones pueden ser utilizados para cualquier transferencia de datos. La Asociación de Industrias del Canal de Fibra, que es el consorcio industrial que promueve el uso del canal de fibra, enumera los siguientes requisitos que éste ambiciona conseguir:

- Enlaces *full-duplex* con dos fibras por enlace.
- Rendimientos desde 100 Mbps hasta 800 Mbps sobre una sola línea (de 200 Mbps a 1.600 Mbps por línea *full-duplex*).
- Cobertura de distancias de hasta 10 km.
- Conectores pequeños.
- Alta capacidad de utilización independiente de la distancia.
- Mayor conectividad que los actuales canales de conexiones múltiples.
- Amplia disponibilidad (es decir, componentes estándar).
- Soporte para múltiples niveles de coste/rendimiento, desde pequeños sistemas hasta grandes computadores.
- Capacidad de transportar varios grupos de órdenes de interfaz para canales y protocolos de red ya existentes.

La solución pasaba por desarrollar un mecanismo de transporte simple y genérico basado en enlaces punto a punto y una red de conmutación. Esta infraestructura subyacente soporta un esquema de codificación y creación de tramas que podría permitir todo un abanico de protocolos de canal y de redes.

ELEMENTOS DEL CANAL DE FIBRA

Los principales elementos de una red de canal de fibra son los sistemas finales, denominados **nodos**, y la red propiamente dicha, que consta de uno o más elementos de conmutación. El conjunto de elementos de conmutación se denomina **estructura**. Estos elementos se encuentran interconectados mediante enlaces punto a punto entre puertos a través de nodos individuales y conmutadores. La comunicación consiste en la transmisión de las tramas a través de los enlaces punto a punto.

Cada nodo incluye uno o más puertos para la interconexión, llamados N_puertos. Análogamente, cada elemento de conmutación de la estructura incluye varios puertos, llamados F_puertos. La interconexión se realiza mediante enlaces bidireccionales entre puertos. Cualquier nodo puede comunicarse con otro nodo conectado a la misma estructura haciendo uso de los servicios de ésta. Todo el encaminamiento de tramas entre N_puertos lo lleva a cabo la estructura. Las tramas se pueden almacenar temporalmente en la estructura, haciendo posible que se conecten a ésta nodos con distintas velocidades de transmisión.

Como se muestra en la Figura 16.10, una estructura puede implementarse como un único elemento de estructura con nodos conectados (una simple disposición en estrella) o como una red más general de elementos de estructura. En cualquier caso, la estructura es responsable del almacenamiento temporal y encaminamiento de tramas entre los nodos origen y destino.

La red de canal de fibra es bastante diferente de las LAN IEEE 802. En contraste con las LAN típicas de medio compartido, el canal de fibra es más parecido a una red tradicional de conmutación de circuitos o de paquetes. Así, no necesita abordar cuestiones de control de acceso al medio. Dado que se basa en una red de conmutación, el canal de fibra se escala fácilmente en términos de N_puertos, velocidad de transmisión de datos y distancia cubierta. Este enfoque proporciona una gran flexibilidad. El canal de fibra se puede acomodar fácilmente a nuevos medios y velocidades de transmisión mediante la incorporación de nuevos conmutadores y F_puertos a una estructura ya existente. Así, una inversión realizada no se pierde ante una actualización a nuevas tecnologías y equipamiento. Además, la arquitectura de protocolos en niveles admite las interfaces de entrada/salida y los protocolos de red existentes, preservando la inversión realizada.

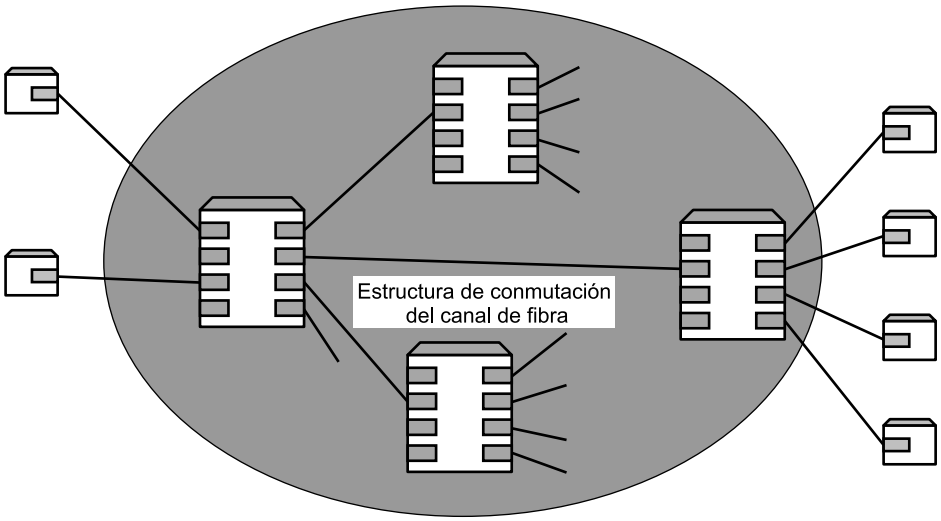


Figura 16.10. Red de canal de fibra.

ARQUITECTURA DE PROTOCOLOS DEL CANAL DE FIBRA

El estándar de canal de fibra se organiza en cinco niveles, definiendo cada uno de ellos una función concreta o un conjunto de funciones relacionadas. El estándar no establece una correspondencia entre niveles y las implementaciones reales, con una interfaz específica entre niveles adyacentes. Es más, el estándar se refiere al nivel como un «artificio documental» usado para agrupar funciones relacionadas entre sí. Las capas son las siguientes:

- **Medio físico FC-0:** incluye fibra óptica para aplicaciones de larga distancia, cable coaxial para altas velocidades a cortas distancias y par trenzado apantallado para bajas velocidades sobre cortas distancias.
- **Protocolo de transmisión FC-1:** define el esquema de codificación de la señal.
- **Protocolo de delimitación FC-2:** incluye las topologías definidas, el formato de trama, el control de flujo y de errores y la agrupación de tramas en entidades lógicas llamadas secuencias y permutas.
- **Servicios comunes FC-3:** incluye la multidifusión.
- **Transformación FC-4:** define la conversión de distintos protocolos de canal y de red a canal de fibra, incluyendo IEEE 802, ATM, IP y la interfaz SCSI.

MEDIOS FÍSICOS Y TOPOLOGÍAS DEL CANAL DE FIBRA

Una de las mayores ventajas del estándar de canal de fibra es que proporciona todo un rango de opciones para el medio físico, su velocidad y la topología de la red (*véase* la Tabla 16.5).

Medios de transmisión

Las opciones sobre el medio de transmisión que están disponibles en el canal de fibra incluyen par trenzado apantallado, cable coaxial de vídeo y fibra óptica. Las velocidades estandarizadas van

Tabla 16.5. Distancia máxima para los distintos tipos de medios de canal de fibra.

	800 Mbps	400 Mbps	200 Mbps	100 Mbps
Fibra de modo simple	10 km	10 km	10 km	—
Fibra multimodo de 50 μm	0,5 km	1 km	2 km	—
Fibra multimodo de 62,5 μm	175 m	1 km	1 km	—
Cable coaxial de vídeo	50 m	71 m	100 m	100 m
Cable coaxial en miniatura	14 m	19 m	28 m	42 m
Par trenzado apantallado	28 m	46 m	57 m	80 m

desde 100 Mbps hasta 3,2 Gbps. Las distancias de los enlaces punto a punto abarcan desde 33 m hasta 10 km.

Topologías

La topología más general soportada por el canal de fibra es la que se conoce como topología conmutada o topología de estructura. Se trata de una topología arbitraria que contiene al menos un conmutador para interconectar una serie de sistemas finales. Esta topología puede también consistir en un número de conmutadores formando una red de conmutación, con algunos de ellos (o todos) dando soporte a los nodos finales.

El encaminamiento en la topología de estructura es transparente a los nodos. Cada puerto en la configuración posee una dirección única. Cuando los datos procedentes de un nodo son transmitidos hacia la estructura, el conmutador al que el nodo de origen está conectado determina la localización del puerto de destino usando la dirección del mismo que se encuentra en la trama de datos. A continuación, el conmutador entrega la trama a otro nodo conectado al mismo conmutador, o bien a un conmutador adyacente para su encaminamiento hacia el destino remoto.

La topología de estructura proporciona escalabilidad de la capacidad: a medida que se añaden puertos adicionales, la capacidad total de la red se incrementa, minimizando así la congestión y la contención e incrementando el rendimiento. La estructura es independiente del protocolo y altamente insensible a problemas de distancia. La tecnología de los conmutadores y de los enlaces de transmisión que los conectan con los nodos pueden ser cambiados sin que este hecho afecte a la configuración global. Otra ventaja de esta topología es que se minimiza la carga en los nodos. Un nodo individual del canal de fibra (un sistema final) es únicamente responsable del manejo de una conexión punto a punto entre él y la estructura; ésta se encarga del encaminamiento entre puertos y de la detección de errores.

Además de la topología de estructura, el estándar del canal de fibra define dos topologías adicionales. Con la topología punto a punto existen solamente dos puertos que se encuentran directamente conectados, sin la intervención de conmutadores en la estructura. En este caso no existe encaminamiento alguno. La topología en bucle arbitrado es una configuración simple y de bajo coste para conectar hasta 126 nodos en un bucle. El bucle arbitrado funciona de una forma ligeramente similar a los protocolos de paso de testigo que han sido estudiados con anterioridad.

Las topologías, los medios de transmisión y las velocidades pueden ser combinados con objeto de proporcionar una configuración optimizada para un determinado sitio. La Figura 16.11 es un ejemplo que ilustra las principales aplicaciones del canal de fibra.

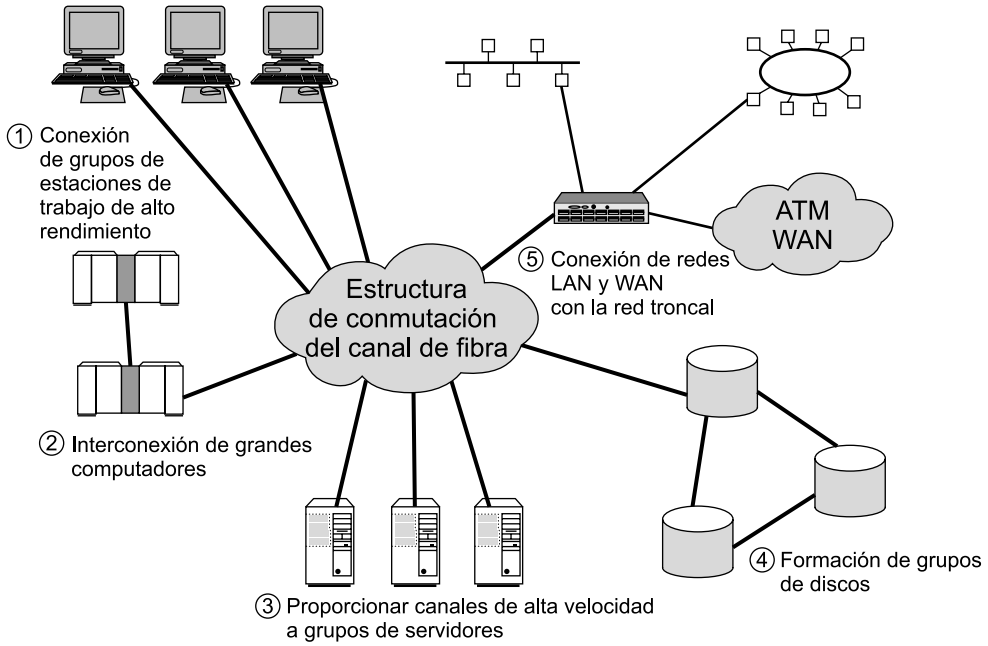

① Conexión de grupos de estaciones de trabajo de alto rendimiento
ATM WAN
⑤ Conexión de redes LAN y WAN con la red troncal
Estructura de conmutación del canal de fibra
② Interconexión de grandes computadores
④ Formación de grupos de discos
③ Proporcionar canales de alta velocidad a grupos de servidores

Figura 16.11. Cinco aplicaciones del canal de fibra.

PERSPECTIVAS DEL CANAL DE FIBRA

El canal de fibra está respaldado por un grupo industrial conocido como la Asociación del Canal de Fibra, encontrándose disponible una gama de tarjetas de red para diferentes aplicaciones. El canal de fibra ha sido principalmente más aceptado como una tecnología mejorada para la interconexión de dispositivos periféricos, proporcionando servicios que podrían reemplazar esquemas como SCSI. Se trata de una solución técnicamente atractiva para los requisitos generales de redes LAN de alta velocidad, pero debe competir con Ethernet y las LAN ATM. El coste y las cuestiones de rendimiento deberían ser los factores cruciales para un gestor a la hora de decidir entre estas tecnologías.

16.5. LECTURAS Y SITIOS WEB RECOMENDADOS

[STAL00] cubre en mayor profundidad todos los sistemas LAN que se han discutido en este capítulo.

[SPUR00] proporciona una visión general concisa pero completa de todos los sistemas 802.3 desde 10 Mbps hasta 1 Gbps, incluyendo algunas indicaciones para la configuración de un solo segmento de cada medio diferente, así como un esbozo de la construcción de Ethernet multisegmento usando diferentes medios de transmisión. Dos tratamientos excelentes de Ethernet a 100 Mbps y Gigabit Ethernet son [SEIF98] y [KADA98]. Un buen artículo de evaluación de Gigabit Ethernet es [FRAZ99]. [10GE02] es un documento técnico que proporciona una introducción muy útil a Ethernet a 10 Gbps.

[SACH96] es una evaluación del canal de fibra. Otro tratamiento corto, aunque útil, es [FCIA01].

10GE02 10 Gigabit Ethernet Alliance. *10 Gigabit Ethernet—Technology Overview*. White paper, abril 2002.

FCIA01 Fibre Channel Industry Association. *Fibre Channel Storage Area Networks*. San Francisco: Fibre Channel Industry Association, 2001.

FRAZ99 Frazier, H., y Johnson, H. «Gigabit Ethernet: From 100 to 1,000 Mpbs.» *IEEE Internet Computing*, enero/febrero 1999.

KADA98 Kadambi, J.; Crayford, I.; y Kalkunte, M. *Gigabit Ethernet*. Upper Saddle River, NJ: Prentice Hall, 1998.

SACH96 Sachs, M., y Varma, A. «Fibre Channel and Related Standards.» *IEEE Communications Magazine*, agosto 1996.

SEIF98 Seifert, R. *Gigabit Ethernet*. Reading, MA: Addison-Wesley, 1998.

SPUR00 Spuergeon, C. *Ethernet: The Definitive Guide.* Cambridge, MA: O'Reilly and Associates, 2000.

STAL00 Stallings, W. *Local and Metropolitan Area Networks*, *Sixth Edition*. Upper Saddle River, NJ: Prentice Hall, 2000.

SITIOS WEB RECOMENDADOS

- **Laboratorio de Interoperabilidad:** sitio de la Universidad de New Hampshire para la evaluación de equipos de LAN de alta velocidad.
- **Sitio web sobre Ethernet de Charles Spurgeon:** contiene información extensa sobre Ethernet, incluyendo enlaces y documentos.
- **Alianza Ethernet 10 Gigabits:** este grupo promueve el estándar Ethernet a 10 Gbps.
- **Asociación de Industrias del Canal de Fibra:** contiene tutoriales, documentos técnicos, enlaces a vendedores y descripciones de aplicaciones del canal de fibra.
- **Asociación de Industrias de Redes de Almacenamiento:** consorcio de industrias de desarrolladores, integradores y profesionales de las TI que promueven tecnologías y soluciones de redes de almacenamiento.

16.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

ALOHA
ALOHA ranurado
acceso múltiple con detección de portadora (CSMA)
acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD)
canal de fibra
colisión

CSMA 1-persistente
CSMA no persistente
CSMA *p*-persistente
espera exponencial binaria
Ethernet
funcionamiento *full-duplex*
red de paso de testigo (en anillo)
red de paso de testigo (en anillo) dedicada (DTR)
repetidor

CUESTIONES DE REPASO

16.1. ¿Qué es una agrupación centralizada de servidores?

16.2. Explique los tres protocolos persistentes que pueden ser usados con CSMA.

16.3. ¿Qué es CSMA/CD?

16.4. Explique el proceso de espera exponencial binaria.

16.5. ¿Cuáles son las opciones de medios de transmisión en Fast Ethernet?

16.6. ¿En qué se diferencia Fast Ethernet de 10BASE-T, además de en la velocidad?

16.7. En el contexto de las redes Ethernet, ¿qué es el funcionamiento *full-duplex*?

16.8. ¿Qué funciones lleva a cabo un repetidor en una red de paso de testigo en anillo?

16.9. ¿Qué diferencias hay entre una red tradicional de paso de testigo y una red de paso de testigo dedicada?

16.10. Enumere los niveles del canal de fibra y las funciones de cada uno de ellos.

16.11. ¿Cuáles son las opciones de topología en el canal de fibra?

16.12. En condiciones de carga elevada, ¿en qué se diferencia el comportamiento de CSMA/CD y una red de paso de testigo?

EJERCICIOS

16.1. Una desventaja de los enfoques de contención en redes LAN, como CSMA/CD, es el desaprovechamiento de la capacidad que se origina debido al intento simultáneo de varias estaciones de acceder al canal. Supóngase que el tiempo se divide en ranuras discretas y que cada una de las N estaciones tiene una probabilidad p de intentar transmitir durante cada ranura. ¿Qué fracción de las ranuras se desaprovecha debido a intentos simultáneos de transmisión?

16.2. Considérese la siguiente situación en el caso de CSMA *p*-persistente. Una estación se encuentra lista para transmitir y está escuchando la transmisión actual. Supongamos que no hay ninguna otra estación lista para transmitir y que no habrá otras transmisiones durante un periodo indefinido de tiempo. Si consideramos que la unidad de tiempo utilizada en el protocolo es T, muéstrese que el número medio de iteraciones del paso 1 del protocolo es $1/p$ y que, por tanto, el tiempo medio que la estación tendrá que esperar después de la transmisión actual es $T\left(\frac{1}{p} - 1\right)$. *Sugerencia:* haga uso de la igualdad

$$\sum_{i=1}^{\infty} iX^{i-1} = \frac{1}{(1-X)^2}$$

16.3. El algoritmo de espera exponencial binaria se define en IEEE 802 como sigue:

El retardo es un múltiplo entero de la duración de una ranura de tiempo. El número de ranuras de tiempo a retrasarse antes de la enésima retransmisión se elige como un entero r aleatorio uniformemente distribuido en el rango $0 \leqslant r < 2^K$, siendo $K = \min(n, 10)$.

La duración de una ranura es, en líneas generales, el doble del tiempo de propagación de ida y vuelta. Suponga que dos estaciones siempre tienen una trama lista para ser enviada. Después de una colisión, ¿cuál es el número medio de intentos de retransmisión antes de que una estación consiga transmitir satisfactoriamente? ¿Cuál es dicho número si se consideran tres estaciones que, al igual que antes, siempre tienen tramas listas para ser transmitidas?

16.4. Describa el patrón de señal producido sobre el medio por el preámbulo de la trama MAC IEEE 802.3 codificada con Manchester.

16.5. Suponga una red LAN en anillo con paso de testigo en la que la estación de destino elimina la trama de datos y envía inmediatamente una confirmación corta al emisor, en lugar de dejar que la trama original vuelva al emisor. ¿Cómo afectará este cambio al rendimiento?

16.6. Otra técnica de control de acceso al medio para redes en anillo es el anillo ranurado (*slotted ring*). En ella existen una serie de ranuras de longitud fija circulando continuamente por el anillo. Cada ranura contiene un bit inicial que indica si la ranura se encuentra llena o no. Una estación que desee transmitir espera hasta que le llegue una ranura vacía, la marca como «llena» e inserta una trama de datos a medida que la ranura circula. A continuación, la ranura realiza una vuelta completa y es marcada de nuevo como «vacía» por la estación que la usó. ¿En qué sentido es este protocolo (paso de testigo ranurado) el complemento del paso de testigo tradicional?

16.7. Considere un anillo ranurado de 10 km de longitud con una velocidad de datos de 10 Mbps y 500 repetidores, cada uno de los cuales introduce un retardo de 1 bit. Cada ranura contiene espacio para albergar una dirección de origen de 1 byte, una dirección de destino de 1 byte, 2 bytes de datos y 5 bits de control, alcanzando así un total de 37 bits. Determine el número de ranuras que hay en el anillo.

16.8. La tasa efectiva de datos con el esquema de codificación 8B6T en un canal simple es de 33 Mbps con una tasa de señalización de 25 Mbaudios. ¿Cuál es la tasa efectiva de datos con una tasa de señalización de 25 Mbaudios si se utiliza un esquema ternario puro?

16.9. Usando una codificación 8B6T, el algoritmo DC niega en ocasiones todos los símbolos ternarios en un grupo de código. ¿Cómo reconoce el receptor que se ha producido este hecho? ¿Cómo discrimina el receptor entre un grupo de código negado y uno que no lo ha sido? Por ejemplo, el grupo de código para el byte de datos 00 es $+-00+-$ y el grupo de código para el byte de datos 38 es su negación, esto es, $-+00-+$.

16.10. Dibuje el diagrama de estados del decodificador MLT que se corresponde con el diagrama de estados del codificador de la Figura 16.12.

16.11. Dibuje la forma de onda del resultado de codificar el flujo de bits 0101110 con NRZ-L, NRZI, Manchester, Manchester Diferencial y MLT-3.

APÉNDICE 16A. CODIFICACIÓN DE SEÑALES DIGITALES PARA REDES LAN

En el Capítulo 5 vimos algunas de las técnicas usuales de codificación de datos digitales para transmisión, incluyendo Manchester y Manchester diferencial, que se usan en algunos estándares LAN. En este apéndice examinaremos algunos esquemas de codificación adicionales citados en este capítulo.

4B/5B-NRZI

Este esquema, que es realmente una combinación de dos algoritmos de codificación, se usa tanto en 100BASE-X como en FDDI. Para comprender el significado de esta elección consideremos primero el sencillo esquema de codificación NRZ (no retorno a cero). Con NRZ, un estado de señal representa un uno binario y otro estado de señal un cero binario. El inconveniente de esta aproximación es la ausencia de sincronismo. Dado que las transiciones en el medio resultan impredecibles, no hay forma de que el receptor sincronice su reloj con el del emisor. Una solución a este problema es codificar los datos binarios de forma que se garantice la presencia de transiciones. Por ejemplo, los datos se podrían codificar primero empleando la codificación Manchester. La desventaja de esta aproximación es que la eficiencia es sólo del 50 por ciento. Es decir, debido a que pueden existir nada menos que dos transiciones por intervalo de bit, se necesita una velocidad de señalización de 200 millones de elementos de señal por segundo (200 Mbaudios) para conseguir una velocidad de transmisión de 100 Mbps. Esto representa un coste y una carga técnica innecesarios.

Se puede conseguir una eficiencia superior haciendo uso del código 4B/5B, en el cual la codificación se realiza en cada momento sobre 4 bits. Cada 4 bits de datos se codifican en un símbolo con cinco *bits de código*, de modo que cada bit de código contiene un único elemento de señal. El bloque de cinco bits de código se llama *grupo de código*. En efecto, cada grupo de 4 bits se codifica como 5 bits. La eficiencia se incrementa así hasta el 80 por ciento: se consiguen 100 Mbps con 125 Mbaudios.

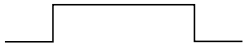
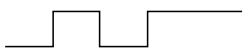
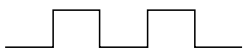
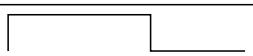
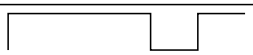
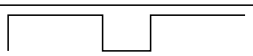
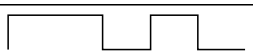
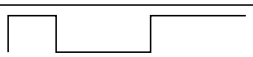
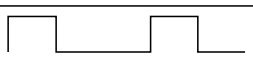
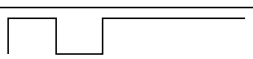
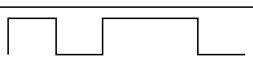
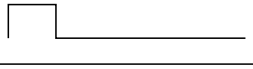
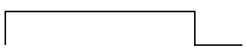
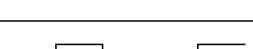
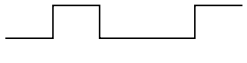
Para asegurar la sincronización se lleva a cabo un segundo paso de codificación: cada bit de código de la secuencia 4B/5B se trata como un valor binario y se codifica usando la técnica de no retorno a cero invertido (NRZI) (*véase* Figura 5.2). En este código, un 1 binario se representa como una transición al principio del intervalo de bit y un 0 binario sin transición al comienzo del intervalo de bit; es decir, no hay transiciones. La ventaja de NRZI es que emplea codificación diferencial. Recordemos del Capítulo 5 que en codificación diferencial la señal se decodifica comparando la polaridad de elementos de señal adyacentes, en lugar del valor absoluto de un elemento de señal. Una ventaja de este esquema es que, en presencia de ruido y distorsión, resulta generalmente más fácil detectar una transición que comparar un valor con un umbral.

Ahora estamos en condiciones de describir el código 4B/5B y de comprender las decisiones tomadas. En la Tabla 16.6 se muestra la codificación de símbolos. Se muestra cada patrón de grupo de código de 5 bits junto con la realización NRZI. Dado que se codifican cuatro bits con un patrón de 5 bits, sólo se necesitan 16 de los 32 patrones posibles para la codificación de los datos. Los códigos seleccionados para representar los 16 bloques de datos de 4 bits son tales que existen al menos dos transiciones para cada código de grupo de 5 bits. No se permiten más de tres ceros en una fila a lo largo de uno o más grupos de código:

El esquema de codificación se puede resumir como sigue:

1. Se rechaza la realización de una simple codificación NRZ dado que no proporciona sincronismo; no aparecen transiciones en una secuencia de unos y ceros.

Tabla 16.6. Grupos de código 4B/5B

Datos de entrada (4 bits)	Grupo de código (5 bits)	Patrón NRZI	Interpretación
0000	11110		Dato 0
0001	01001		Dato 1
0010	10100		Dato 2
0011	10101		Dato 3
0100	01010		Dato 4
0101	01011		Dato 5
0110	01110		Dato 6
0111	01111		Dato 7
1000	10010		Dato 8
1001	10011		Dato 9
1010	10110		Dato A
1011	10111		Dato B
1100	11010		Dato C
1101	11011		Dato D
1110	11100		Dato E
1111	11101		Dato F
	11111		Libre
	11000		Comienzo de delimitador de secuencia, parte 1
	10001		Comienzo de delimitador de secuencia, parte 2
	01101		Fin de delimitador de secuencia, parte 1
	00111		Fin de delimitador de secuencia, parte 2
	00100		Error de transmisión
	Otro		Códigos no válidos

2. Los datos a transmitir deben ser primero codificados para asegurar la existencia de transiciones. Se elige el código 4B/5B frente a Manchester porque es más eficiente.
3. El código 4B/5B se codifica posteriormente usando NRZI, de modo que la señal diferencial resultante mejorará la fiabilidad en la recepción.
4. Los patrones de 5 bits específicamente elegidos para la codificación de los 16 patrones de datos de 4 bits se seleccionan con el fin de garantizar la existencia de no más de tres ceros en una fila con objeto de conseguir una sincronización adecuada.

Los grupos de código no empleados para representar datos se declaran como no válidos o se les asigna un significado especial como símbolos de control. Estas asignaciones se enumeran en la Tabla 16.6. Los símbolos de no datos se encuadran en las siguientes categorías:

- **Libre:** el grupo de código libre se transmite entre secuencias de transmisión de datos. Consiste en un flujo constante de unos binarios, lo que se traduce con NRZI en un cambio continuo entre dos niveles de señal. Este patrón de relleno continuo establece y mantiene la sincronización y se usa en el protocolo CSMA/CD para indicar que el medio compartido se encuentra libre.
- **Comienzo de delimitador de secuencia:** se utiliza para delimitar el comienzo de una secuencia de transmisión de datos; consta de dos grupos de código diferentes.
- **Final de delimitador de secuencia:** empleado como fin de las secuencias de transmisión de datos normales; consta de dos grupos de código diferentes.
- **Error de transmisión:** este grupo de código se interpreta como un error de señalización. El uso normal de este indicador se establece en repetidores con el fin de propagar errores recibidos.

MLT-3

Aunque 4B/5B es efectivo para fibra óptica, no resulta tan apropiado como lo es para par trenzado. El motivo de este hecho es que la energía de la señal se concentra de manera que se producen emisiones de radiación no deseadas desde el cable. MLT-3, que se usa tanto en 100BASE-TX como en la versión de par trenzado de FDDI, está diseñado para solucionar este problema.

Se siguen los siguientes pasos:

1. **Conversión NRZI a NRZ.** La señal 4B/5B-NRZI de la 100BASE-X básica se convierte de nuevo a NRZ.
2. **Aleatorización.** Se entremezcla la secuencia de bits para producir una distribución de espectro más uniforme para el siguiente paso.
3. **Codificador.** La secuencia de bits mezclados se codifica usando el esquema conocido como MLT-3.
4. **Controlador.** Se transmite la codificación resultante.

El efecto del esquema MLT-3 es concentrar la mayor parte de la energía en la señal transmitida por debajo de los 30 MHz, lo que reduce las emisiones. Esto disminuye los problemas debidos a interferencias.

La codificación MLT-3 produce una salida que tiene una transición para cada uno binario y que usa tres niveles: una tensión positiva ($+V$), una negativa ($-V$) y ausencia de ésta (0). Las

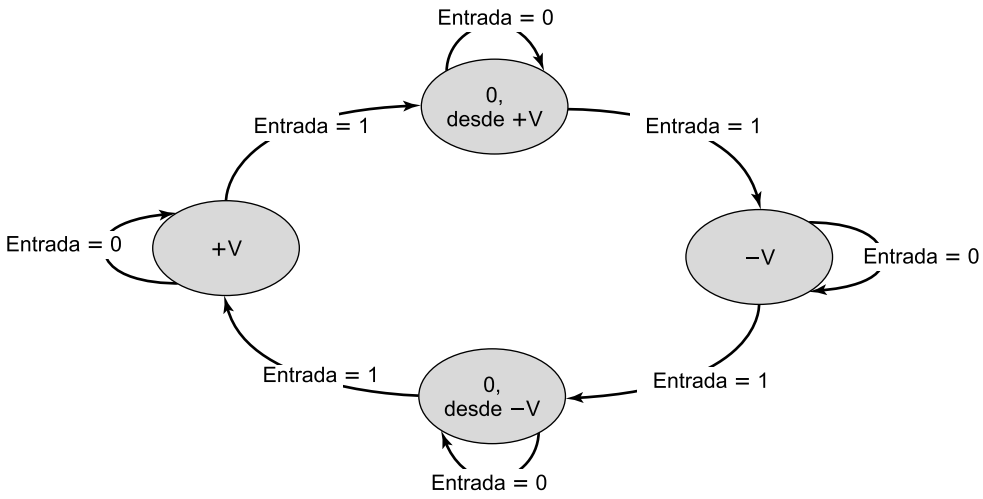


Figura 16.12. Diagrama de estados del codificador MLT-3.

reglas de codificación se explican mejor con ayuda del diagrama de estados del codificador mostrado en la Figura 16.12:

1. Si el siguiente bit de entrada es cero, el siguiente valor de salida es el mismo que el valor precedente.
2. Si el siguiente bit de entrada es un uno, el siguiente valor de salida implica una transición:
   a) Si el valor de salida anterior fue $+V$ o $-V$, el siguiente valor de salida es 0.
   b) Si el valor de salida precedente fue 0, el siguiente valor de salida es distinto de cero, y de signo opuesto al de la última salida distinta de cero.

En la Figura 16.13 se muestra un ejemplo. Cada vez que haya un 1 de entrada, existe una transición. Se alterna la aparición de $+V$ y $-V$.

8B6T

El algoritmo de codificación 8B6T utiliza señalización ternaria. Con este tipo de señalización, cada elemento de señal puede tomar uno de tres valores posibles (tensión positiva, tensión negativa y tensión nula). Un código ternario puro es aquel en que se aprovecha la capacidad de transportar información de una señal ternaria. Sin embargo, este tipo de código no resulta atractivo por las mismas razones por las que se desestima un código binario puro (NRZ): ausencia de sincronización. A pesar de ello, existen esquemas denominados *métodos de codificación por bloques* que se

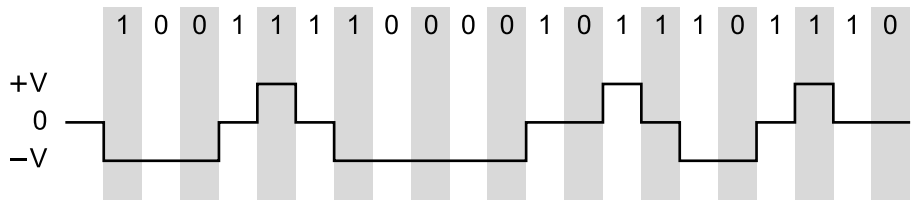


Figura 16.13. Ejemplo de codificación MLT-3.

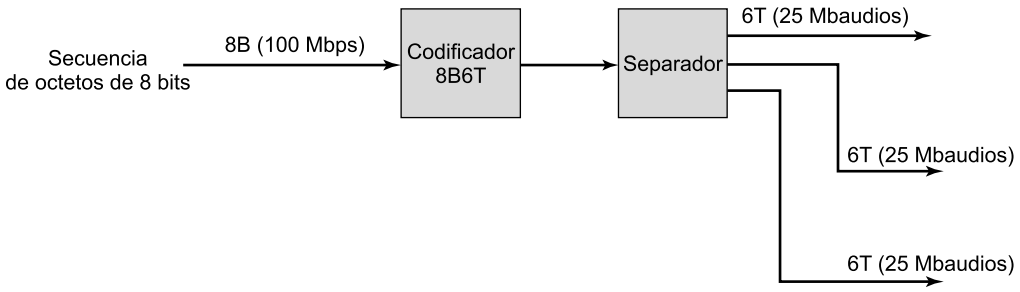


Figura 16.14. Esquema de transmisión 8B6T.

aproximan a la eficiencia de un código ternario y solventan este inconveniente. En 100BASE-T4 se usa un nuevo esquema de codificación por bloques conocido como 8B6T.

En 8B6T, los datos a transmitir se gestionan en bloques de 8 bits. Cada uno de estos bloques se transforma en un grupo de código de 6 símbolos ternarios. La secuencia de grupos de código se transmite después a través de los tres canales de salida siguiendo el esquema de rotación circular (*véase* Figura 16.14). De esta forma, la velocidad de transmisión de datos en cada canal de salida es:

$$\frac{6}{8} \times 33\,\frac{1}{3} = 25 \text{ Mbaudios}$$

En la Tabla 16.7 se muestra una parte de la tabla de código 8B6T; la tabla completa transforma todos los patrones de 8 bits posibles en un único grupo de código de 6 símbolos ternarios. La transformación se elige en base a dos requisitos: sincronización y compensación de tensión continua (DC). Para sincronización, los códigos se seleccionan para maximizar el número medio de transiciones por grupo de código. El segundo requisito consiste en mantener compensada la DC, de modo que la tensión promedia en la línea sea cero. Con este objetivo, todos los grupos de código

Tabla 16.7. Porción de la tabla de código 8B6T.

Octeto de datos	Grupo de código 6T	Octeto de datos	Grupo de código 6T	Octeto de datos	Grupo de código 6T	Octeto de datos	Grupo de código 6T
00	+−00+−	10	+0+−−0	20	00−++−	30	+−00−+
01	0+−+−0	11	++0−0−	21	−−+00+	31	0+−−+0
02	+−0+−0	12	+0+−0−	22	++−0+−	32	+−0−+0
03	−0++−0	13	0++−0−	23	++−0−+	33	−0+−+0
04	−0+0+−	14	0++−−0	24	00+0−+	34	−0+0−+
05	0+−−0+	15	++00−−	25	00+0+−	35	0+−+0−
06	+−0−0+	16	+0+0−−	26	00−00+	36	+−0+0−
07	−0+−0+	17	0++0−−	27	−−++−+	37	−0++0−
08	−+00+−	18	0+−0+−	28	−0−++0	38	−+00−+
09	0−+++−0	19	0+−0−+	29	−−0+0+	39	0−+−+0
0A	−+0+−0	1A	0+−+++−	2A	−0−+0+	3A	−+0−+0
0B	+0−+−0	1B	0+-00+	2B	0−−+0+	3B	+0−−+0
0C	+0−0+−	1C	0−+00+	2C	0−−++0	3C	+0−0−+
0D	0−+−0+	1D	0−++++−	2D	−−00++	3D	0−++0−
0E	−+0−0+	1E	0−+0−+	2E	−0−0++	3E	−+0+0−
0F	+0−−0+	1F	0−+0+−	2F	0−−0++	3F	+0−+0−

seleccionados tienen un número igual de símbolos positivos y negativos o un superávit de un símbolo positivo. Para mantener el equilibrio se usa un algoritmo de compensación DC. Esencialmente, este algoritmo supervisa el peso acumulado de todos los grupos de código transmitidos a través de un par individual. Cada grupo de código tiene un peso 0 o 1. Para compensar, el algoritmo puede negar un grupo de código transmitido (cambia todos los símbolos + por símbolos − y todos los − por +), de forma que el peso acumulado al final de cada grupo de código es siempre 0 o 1.

8B/10B

El esquema de codificación usado en canal de fibra y en Gigabit Ethernet es 8B/10, en el que cada 8 bits de datos se transforman en 10 bits para su transmisión. Este esquema sigue una filosofía similar al esquema 4B/5B empleado en FDDI discutido anteriormente. El esquema 8B/10B se desarrolló y patentó por IBM para su uso en su sistema interconectado ESCON a 200 Mbaudios [WIDM83]. Este esquema es más potente que el 4B/5B en términos de características de transmisión y capacidad de detección de errores.

Los diseñadores de este código enumeran las siguientes ventajas:

- Se puede implementar utilizando transceptores relativamente sencillos y fiables de bajo coste.
- Presenta una buena compensación, con mínimas desviaciones en la ocurrencia de un número igual de bits 0 y 1 a lo largo de una secuencia.
- Proporciona una buena densidad de transiciones para una fácil recuperación del sincronismo.
- Proporciona una capacidad útil de detección de errores.

El código 8B/10B es un ejemplo del código más general *m*B*n*B, en el que *m* bits originales se transforman en *n* bits binarios para la transmisión. Haciendo $n > m$ se introduce redundancia en el código para proporcionar las características de transmisión deseadas.

El código 8B/10B realmente combina otros dos códigos, un código 5B/6B y otro 3B/4B. El uso de estos dos códigos es simplemente un artificio para simplificar la definición de la transformación y de la implementación: la transformación podía haberse definido directamente como un código 8B/10B. En cualquier caso, se define una transformación que traduce cada uno de los posibles bloques originales de 8 bits en un bloque de código de 10 bits. También existe una función llamada *control de disparidad*. Esencialmente, esta función hace un seguimiento del exceso de ceros frente a unos o de unos frente a ceros. La existencia de exceso en un sentido se conoce como disparidad. Si existe disparidad, y si el bloque de código actual aumenta ésta, el bloque de control de disparidad complementa el bloque de código de 10 bits. Esto tiene el efecto de eliminar la disparidad o, al menos, cambiarla de sentido con respecto a la actual.

APÉNDICE 16B. ANÁLISIS DE PRESTACIONES

La elección de una arquitectura LAN o MAN depende de varios factores, siendo la eficiencia uno de los más importantes. Una cuestión relevante es el comportamiento (rendimiento, tiempo de respuesta) de la red ante la existencia de alta carga. En este apéndice se presenta una introducción a este tema, pudiéndose encontrar en [STAL00] una discusión más detallada del mismo.

EFECTO DEL RETARDO DE PROPAGACIÓN Y LA VELOCIDAD DE TRANSMISIÓN

En el Capítulo 7 se introdujo el parámetro a, definido como

$$a = \frac{\text{Tiempo de propagación}}{\text{Tiempo de transmisión}}$$

En este contexto, nos centraremos en un enlace punto a punto, con un tiempo de propagación específico entre dos extremos y un tiempo de transmisión para una trama de tamaño fijo o promedio. Se mostró que el parámetro a se puede expresar como:

$$a = \frac{\text{Longitud del enlace de datos en bits}}{\text{Longitud de la trama en bits}}$$

Este parámetro es también importante en el contexto de redes LAN y MAN, y determina un límite superior para la utilización. Consideremos un mecanismo de acceso completamente eficiente que permita sólo una transmisión en un instante de tiempo dado. Tan pronto como finaliza una transmisión, comienza a transmitir otra estación. Además, la transmisión es sólo de datos, sin bits suplementarios. ¿Cuál es la máxima utilización de red posible? Ésta se puede expresar como la relación entre el rendimiento total de la red y su velocidad:

$$U = \frac{\text{Rendimiento}}{\text{Velocidad}} \tag{16.1}$$

Definamos ahora, como en el Capítulo 7,

R = Velocidad del canal.
d = Distancia máxima ente cualesquiera dos estaciones.
V = Velocidad de propagación de la señal.
L = Longitud media o fija de trama.

El rendimiento es el número de bits transmitidos por unidad de tiempo. Una trama contiene L bits, y la cantidad de tiempo dedicado a esta trama es el tiempo de transmisión real (L/R) más el retardo de propagación (d/V). De este modo,

$$\text{Rendimiento} = \frac{L}{d/V + L/R} \tag{16.2}$$

Pero, por la definición anterior de a:

$$a = \frac{d/V}{L/R} = \frac{Rd}{LV} \tag{16.3}$$

Sustituyendo (16.2) y (16.3) en (16.1):

$$U = \frac{1}{1 + a} \tag{16.4}$$

Obsérvese que esta expresión es diferente de la Ecuación (7.4) dada en el Apéndice 7A. Este hecho se debe a que la última considera un protocolo *half-dúplex* (no se usan tramas de datos con incorporación de confirmación).

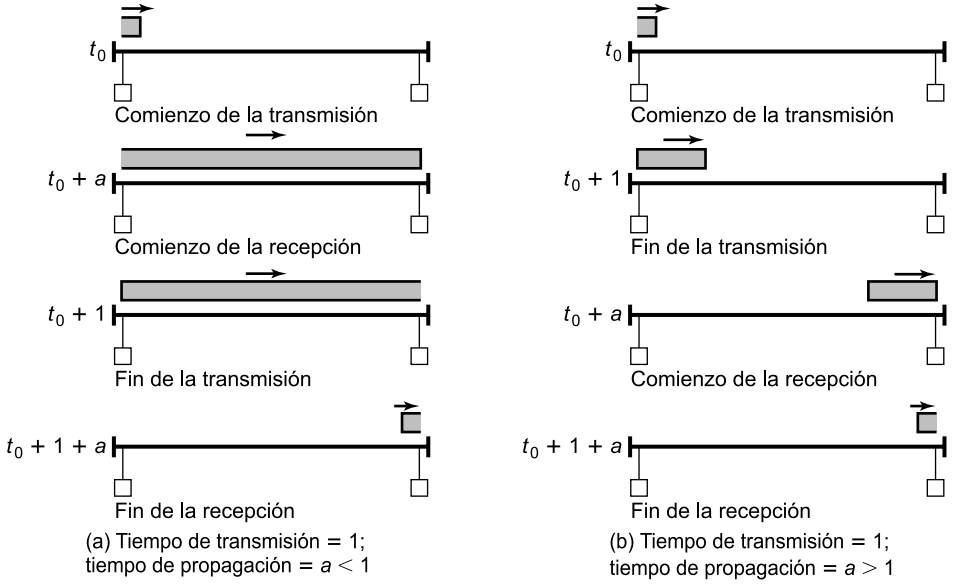


Figura 16.15. Efecto del parámetro *a* en la utilización en un bus en banda base.

Por tanto, la utilización depende de a, lo que se puede comprender intuitivamente estudiando la Figura 16.15. En ella se muestra un bus de banda base con dos estaciones tan distantes como es posible (peor caso) que se turnan en el envío de tramas. Si normalizamos el tiempo de forma que el de transmisión de trama sea 1, el tiempo de propagación es a. Para $a < 1$, la secuencia de eventos es como sigue:

1. Una estación comienza a transmitir en t_0.
2. La recepción empieza en $t_0 + a$.
3. La transmisión se completa en $t_0 + 1$.
4. La recepción finaliza en $t_0 + 1 + a$.
5. La otra estación comienza a transmitir.

Los eventos 2 y 3 se intercambian para $a > 1$. En ambos casos, el tiempo total para un «turno» es $1 + a$, pero el tiempo de transmisión es sólo 1, por lo que la utilización será $1/(1 + a)$.

Lo mismo ocurre en el caso de la red en anillo de la Figura 16.16. Aquí suponemos que una estación transmite y después espera a recibir su propia transmisión antes de que otra estación pueda transmitir. Se sigue la misma secuencia de eventos que anteriormente.

Los valores típicos de a se encuentran en el rango comprendido entre 0,01 y 0,1 para redes LAN y entre 0,1 y muy por encima de 1,0 para redes MAN. En la Tabla 16.8 se muestran algunos valores representativos para una topología en bus. Como se puede ver, la utilización decae para redes mayores y/o con velocidades superiores. Por esta razón desaparece la restricción de una sola trama para redes LAN como FDDI.

Por último, el análisis anterior supone un protocolo «perfecto» en el que se puede transmitir una nueva trama tan pronto como se reciba la trama anterior. En la práctica, el protocolo MAC añade bits suplementarios que hacen que empeore la utilización. Esto se demuestra en el siguiente apartado para las técnicas de paso de testigo y CSMA/CD.

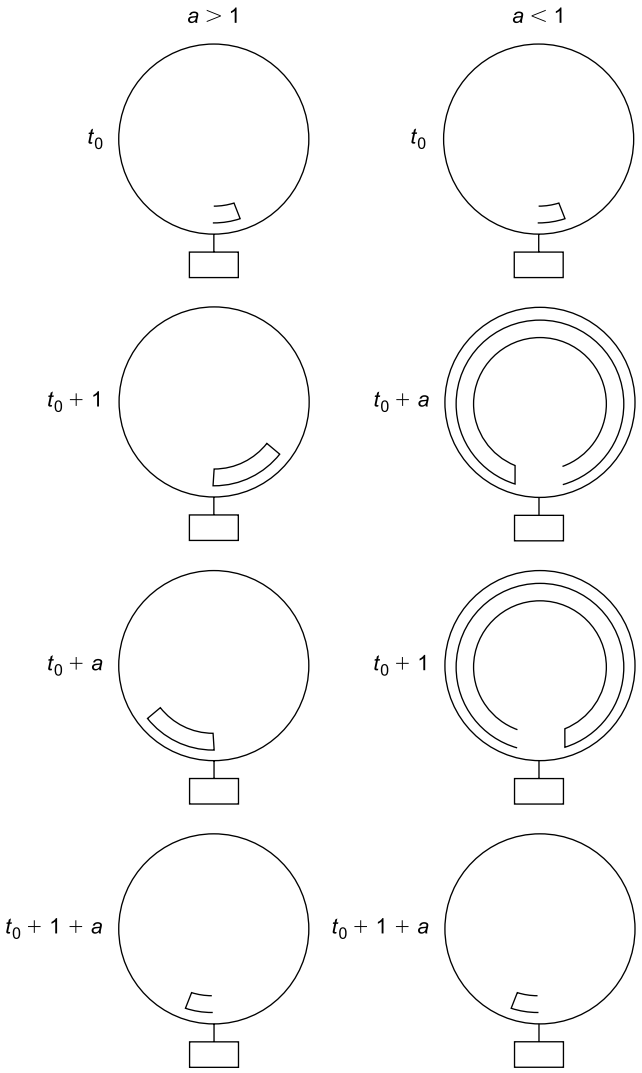


Figura 16.16. Efecto del parámetro *a* en la utilización en una red en anillo.

Tabla 16.8. Valores representativos de *a*.

Velocidad (Mbps)	Tamaño de trama (bits)	Longitud de la red (km)	*a*	1/(1 + *a*)
1	100	1	0,05	0,95
1	1.000	10	0,05	0,95
1	100	10	0,5	0,67
10	100	1	0,5	0,67
10	1.000	1	0,05	0,95
10	1.000	10	0,5	0,67
10	10.000	10	0,05	0,95
100	35.000	200	2,8	0,26
100	1.000	50	25	0,04

MODELOS SENCILLOS DE EFICIENCIA PARA LAS TÉCNICAS DE PASO DE TESTIGO Y CSMA/CD

El objetivo de este apartado es proporcionar al lector una visión de las prestaciones relativas de los protocolos LAN más importantes —CSMA/CD, bus con paso de testigo y anillo con paso de testigo— mediante el desarrollo de dos modelos sencillos de prestaciones. Esperamos que este ejercicio ayude a comprender los resultados de análisis más rigurosos.

En estos modelos se supone una red local con N estaciones activas y un retardo de propagación normalizado máximo igual a a. Para simplificar el análisis se supone que cada estación está siempre lista para transmitir una trama, lo que nos permite desarrollar una expresión para la utilización máxima alcanzable (U). Aunque no se debería analizar la utilización como la única característica destacable de una red local, este parámetro es el más analizado y permite realizar comparaciones útiles acerca de prestaciones.

En primer lugar, consideremos una red en anillo con paso de testigo. El tiempo consumido en el anillo se distribuye entre la transmisión de tramas de datos y el paso del testigo. Denominemos ciclo a la transmisión de una única trama de datos seguida por un testigo y definamos:

C = Tiempo promedio de un ciclo.

T_1 = Tiempo promedio para transmitir una trama de datos.

T_2 = Tiempo promedio en el paso del testigo.

Debería estar claro que la razón de ciclo media es $1/C = 1/(T1 + T2)$. Intuitivamente,

$$U = \frac{T_1}{T_1 + T_2} \tag{16.5}$$

Es decir, el rendimiento, normalizado a la capacidad del sistema, es la fracción de tiempo consumido en la transmisión de los datos.

Centrémonos ahora en la Figura 16.16. El tiempo se normaliza de manera que el tiempo de transmisión de trama es igual a 1 y el tiempo de propagación es a. Obsérvese que el tiempo de propagación debe incluir los retardos de los repetidores. Para el caso $a < 1$ una estación transmite una trama en t_0, recibe la cabecera de su propia trama en $t_0 + a$ y completa la transmisión en $t_0 + 1$. La estación transmite entonces un testigo, lo que implica un tiempo promedio a/N hasta alcanzar la siguiente estación. Así, un ciclo dura $1 + a/N$ y el tiempo de transmisión es 1. Por tanto, $U = 1/(1 + a/N)$.

El razonamiento es ligeramente diferente para el caso $a > 1$. Una estación transmite en t_0, finaliza la transmisión en $t_0 + 1$ y recibe la cabecera de su trama en $t_0 + a$. En este momento se encuentra en condiciones de emitir un testigo, lo que implica un tiempo promedio a/N hasta alcanzar la siguiente estación. En consecuencia, el tiempo de ciclo es $a + a/N$ y $U = 1/(a(1 + 1/N))$.

En resumen,

$$\textbf{Anillo con paso de testigo:} \quad U = \begin{cases} \dfrac{1}{1 + a/N} & a < 1 \\ \dfrac{1}{a(1 + 1/N)} & a > 1 \end{cases} \tag{16.6}$$

Consideremos para CSMA/CD el tiempo organizado en ranuras temporales de duración igual a dos veces el retardo de propagación extremo a extremo. Esto es una forma adecuada para considerar la actividad en el medio; la ranura temporal es igual al tiempo máximo necesario para detectar una colisión desde el inicio de la transmisión. Suponemos de nuevo que existen N estaciones activas. Está claro que si todas las estaciones tienen siempre una trama que transmitir, y lo hacen, no habrá más que colisiones en el medio. Por tanto, supongamos que cada estación limita con una probabilidad P su transmisión durante una ranura disponible.

El tiempo en el medio consta de dos tipos de intervalos. El primero es un intervalo de transmisión, de duración $1/2a$ ranuras. El segundo es un intervalo de contención, que es una secuencia de ranuras en las que se produce colisión o no existe transmisión. El rendimiento es la proporción de tiempo consumido en intervalos de transmisión (similar al razonamiento de la Ecuación (16.5)).

Para determinar la longitud promedio de un intervalo de contención, comenzamos calculando A, la probabilidad de que exactamente una estación intente llevar a cabo una transmisión en una ranura y, en consecuencia, consiga el medio. Ésta es la probabilidad binomial de que cualquier estación intente transmitir y las otras no:

$$A = \binom{N}{1} P^1(1 - P)^{N-1} = NP(1 - P)^{N-1}$$

Esta función alcanza un máximo en P cuando $P = 1/N$:

$$A = (1 - 1/N)^{N-1}$$

Estamos interesados en el máximo porque deseamos calcular el rendimiento máximo del medio. Debe quedar claro que éste se conseguirá si maximizamos la probabilidad de conseguir el medio con éxito. Esto implica que se debe forzar el cumplimiento de la siguiente regla: durante periodos de gran uso, una estación debería restringir su carga ofrecida a $1/N$, (esto supone que cada estación conoce el valor de N). Con el fin de obtener una expresión para el máximo rendimiento posible, se considera válida esta suposición.) Por otra parte, durante periodos de tiempo de poco uso no se puede alcanzar la utilización máxima dado que la carga es demasiado pequeña; esta situación no resulta de interés para nuestros objetivos actuales.

Ahora podemos estimar la longitud media de un intervalo de contención, w, en ranuras:

$$E[w] = \sum_{i=1}^{\infty} i \times \Pr\left[\begin{array}{c}\text{secuencia con } i \text{ ranuras con una colisión} \\ \text{o no transmisión, seguida por una ranura} \\ \text{con una transmisión}\end{array}\right] = \sum_{i=1}^{\infty} i(1 - A)^i A$$

La sumatoria converge a

$$E[w] = \frac{1 - A}{A}$$

Ahora se puede determinar la utilización máxima, que no es más que la longitud del intervalo de transmisión con respecto a un ciclo que consta del intervalo de transmisión y de otro de contención:

$$\textbf{CSMA/CD:} \quad U = \frac{1/2a}{1/2a + (1 - A)/A} = \frac{1}{1 + 2a(1 - A)/A} \tag{16.7}$$

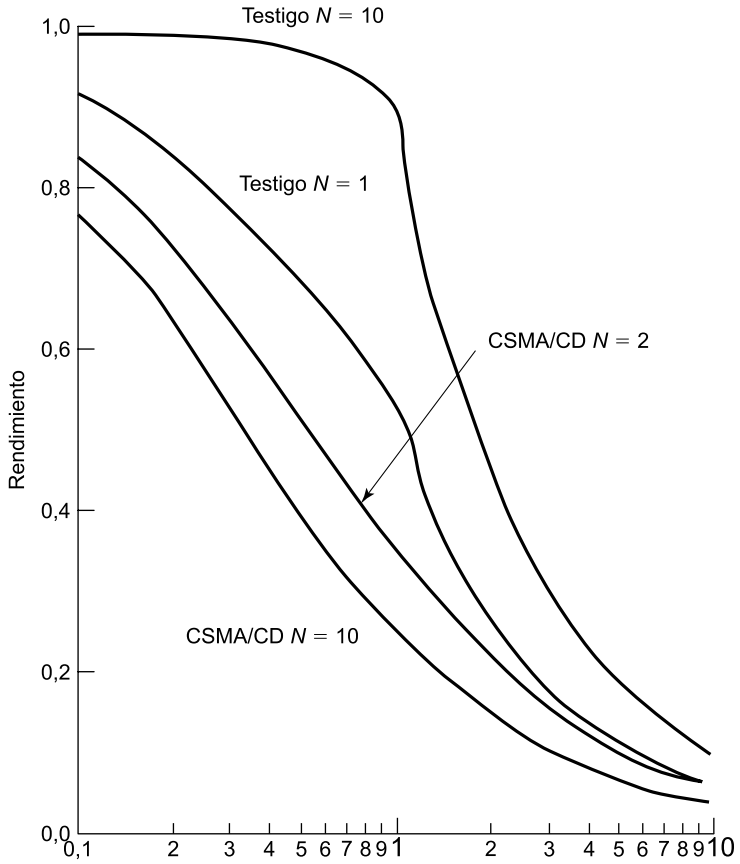


Figura 16.17. Rendimiento en función de *a* para las técnicas de paso de testigo y CSMA/CD.

En la Figura 16.17 se muestra el rendimiento normalizado como función de a para varios valores de N para las técnicas de paso de testigo y CSMA/CD. En ambos protocolos, el rendimiento decrece a medida que aumenta el parámetro a. Este resultado era de esperar, pero la gran diferencia entre los dos protocolos se muestra en la Figura 16.18, que representa el rendimiento en función de N. Las prestaciones de la técnica de paso de testigo mejoran en función de N, ya que se consume menos tiempo en el paso del testigo. Por el contrario, las prestaciones de la técnica CSMA/CD decrecen debido al incremento en la probabilidad de colisión o no transmisión.

Es interesante observar el comportamiento asintótico de U a medida que aumenta N.

$$\textbf{Paso de Testigo:} \quad \lim_{N \to \infty} U = \begin{cases} 1 & a < 1 \\ \dfrac{1}{a} & a > 1 \end{cases} \tag{16.8}$$

Para CSMA/CD debemos saber que $\lim (1 - 1/N)^{N-1} = 1/e$. Por tanto, tenemos que:

$$\textbf{CSMA/CD:} \quad \lim_{N \to \infty} U = \frac{1}{1 + 3{,}44a} \tag{16.9}$$

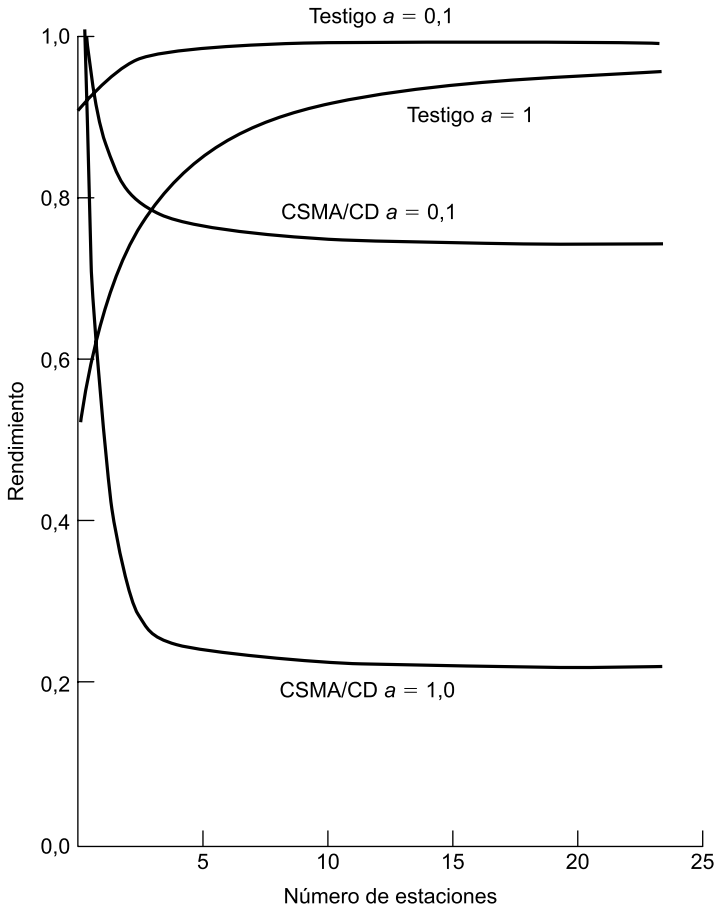


Figura 16.18. Rendimiento en función de *N* para las técnicas de paso de testigo y CSMA/CD.

CAPÍTULO 17

Redes LAN inalámbricas

17.1. Visión general
Aplicaciones de las redes LAN inalámbricas
Requisitos de las redes LAN inalámbricas

17.2. Tecnología LAN inalámbrica
Redes LAN de infrarrojos
Redes LAN de espectro expandido
Redes LAN de microondas de banda estrecha

17.3. Arquitectura y servicios de IEEE 802.11
Arquitectura de IEEE 802.11
Servicios de IEEE 802.11

17.4. Control de acceso al medio en IEEE 802.11
Entrega fiable de datos
Control de acceso
Trama MAC

17.5. Capa física de IEEE 802.11
Capa física original de IEEE 802.11
IEEE 802.11a
IEEE 802.11b
IEEE 802.11g

17.6. Lecturas y sitios web recomendados

17.7. Términos clave y cuestiones de repaso
Términos clave
Cuestiones de repaso

CUESTIONES BÁSICAS

- Las principales tecnologías usadas en redes LAN inalámbricas son los infrarrojos, el espectro expandido y las microondas de banda estrecha.
- El estándar IEEE 802.11 define un conjunto de servicios y diferentes opciones de medios de transmisión para redes LAN inalámbricas.
- Los servicios recogidos en IEEE 802.11 incluyen la gestión de las asociaciones, la entrega de datos y las cuestiones de seguridad.
- La capa física de IEEE 802.11 comprende el uso de infrarrojos y de espectro expandido y ofrece diversas velocidades de datos.

En los últimos años las LAN inalámbricas han ocupado un importante lugar en el mercado de las redes de área local. Cada vez más, las organizaciones se han dado cuenta de que las LAN inalámbricas son un complemento indispensable a las redes cableadas a fin de satisfacer las necesidades de movilidad, traslados, trabajo en red *ad hoc* y cobertura de lugares difíciles de cablear.

Este capítulo examina las redes LAN inalámbricas, comenzando con una visión general de la motivación que ha conducido a ellas y resumiendo los distintos enfoques que se encuentran actualmente en uso. En la siguiente sección se exponen los tres tipos principales de redes LAN inalámbricas, clasificadas de acuerdo con la tecnología de transmisión que utilizan: infrarrojos, espectro expandido y microondas de banda estrecha.

La especificación más notable de redes LAN inalámbricas fue desarrollada por el grupo de trabajo IEEE 802.11. Este estándar será tratado en los contenidos restantes del capítulo.

17.1. VISIÓN GENERAL

Como su propio nombre indica, una red LAN inalámbrica es aquella que hace uso de un medio de transmisión inalámbrico. Hasta hace relativamente poco tiempo, las redes LAN inalámbricas eran poco usadas debido a su alto precio, la baja velocidad de transmisión, la existencia de problemas de seguridad y la necesidad de licencias. A medida que estos problemas se han ido solucionando, la popularidad de las LAN inalámbricas ha crecido rápidamente.

En esta sección se examinan las aplicaciones clave de este tipo de redes, exponiéndose a continuación los requisitos necesarios y las ventajas de su uso.

APLICACIONES DE LAS REDES LAN INALÁMBRICAS

[PAHL95] enumera cuatro áreas de aplicación para las redes LAN inalámbricas: ampliación de redes LAN, interconexión de edificios, acceso nómada y redes *ad hoc*. A continuación se analizan todas ellas.

Ampliación de redes LAN

Los primeros productos de LAN inalámbricas, aparecidos a finales de los años ochenta, eran ofrecidos como sustitutos de las redes LAN cableadas tradicionales. Una red LAN inalámbrica evita el coste de la instalación del cableado y facilita las tareas de traslado y otras modificaciones en la estructura de la red. Sin embargo, esta motivación de las LAN inalámbricas fue superada por los acontecimientos. En primer lugar, a medida que la necesidad de redes LAN se hizo cada vez más patente, los arquitectos incluyeron en el diseño de los nuevos edificios un extenso cableado para aplicaciones de datos. Además, con los avances en la tecnología de transmisión de datos se ha incrementado la dependencia con los pares trenzados para redes LAN, especialmente con los UTP de categoría 3 y categoría 5. Así, dado que la mayor parte de los edificios viejos estaban ya cableados con par trenzado de categoría 3, y muchos de los edificios de nueva construcción lo están con par trenzado de categoría 5, resulta escaso el uso de LAN inalámbricas como sustituto de las LAN cableadas.

Sin embargo, el papel de una LAN inalámbrica como alternativa a las LAN cableadas es importante en un gran número de entornos. Algunos ejemplos son edificios que poseen una gran superficie, como plantas de fabricación, plantas comerciales y almacenes, edificios históricos con insuficiente cable de par trenzado y en los que está prohibido hacer más agujeros para introducir nuevo cableado, y pequeñas oficinas donde la instalación y el mantenimiento de una LAN cableada no resultan rentables. En todos estos casos, una LAN inalámbrica ofrece una alternativa efectiva y más atractiva. En la mayor parte de estas situaciones, una organización dispondrá también de una LAN cableada con servidores y algunas estaciones de trabajo estacionarias. Por ejemplo, una planta de manufacturación dispone, generalmente, de una oficina independiente de la propia planta, pero que debe estar interconectada con ella con el fin de proporcionar trabajo en red. Por tanto, una LAN inalámbrica está conectada en muchas ocasiones con una LAN cableada en el mismo recinto, denominándose este campo de aplicación ampliación o extensión de redes LAN.

En la Figura 17.1 se muestra una configuración sencilla de una LAN inalámbrica típica en muchos entornos. Existe una LAN troncal cableada, como una Ethernet, que conecta varios servidores, estaciones de trabajo y uno o más puentes o dispositivos de encaminamiento para la comunicación con otras redes. Adicionalmente, existe un módulo de control (CM, *Control Module*) que funciona como interfaz con la LAN inalámbrica. El módulo de control incluye funciones propias de un puente o de un dispositivo de encaminamiento para conectar la LAN inalámbrica con la troncal. Además, se incluye algún tipo de lógica de control de acceso, como por ejemplo un esquema de sondeo o uno de paso de testigo, para regular el acceso de los sistemas finales. Hemos de destacar que algunos de los sistemas finales son dispositivos independientes, como estaciones de trabajo y servidores. Los concentradores (*hub*) u otros módulos de usuario (UM, *User Module*) que controlan varias estaciones fuera de una LAN cableada pueden también formar parte de la LAN inalámbrica.

La configuración de la Figura 17.1 se denomina LAN inalámbrica de celda única, ya que todos los sistemas finales inalámbricos se encuentran en el dominio de un único módulo de control. Otra configuración común, sugerida en la Figura 17.2, es una LAN inalámbrica de celdas múltiples. En este caso existen varios módulos de control interconectados por una LAN cableada. Cada módulo de control da servicio a varios sistemas finales inalámbricos dentro de su rango de transmisión. Por ejemplo, con una LAN de infrarrojos, la transmisión se encuentra limitada a una sola habitación, por lo que se necesita una celda en cada habitación de un edificio de oficinas que precise de soporte inalámbrico.

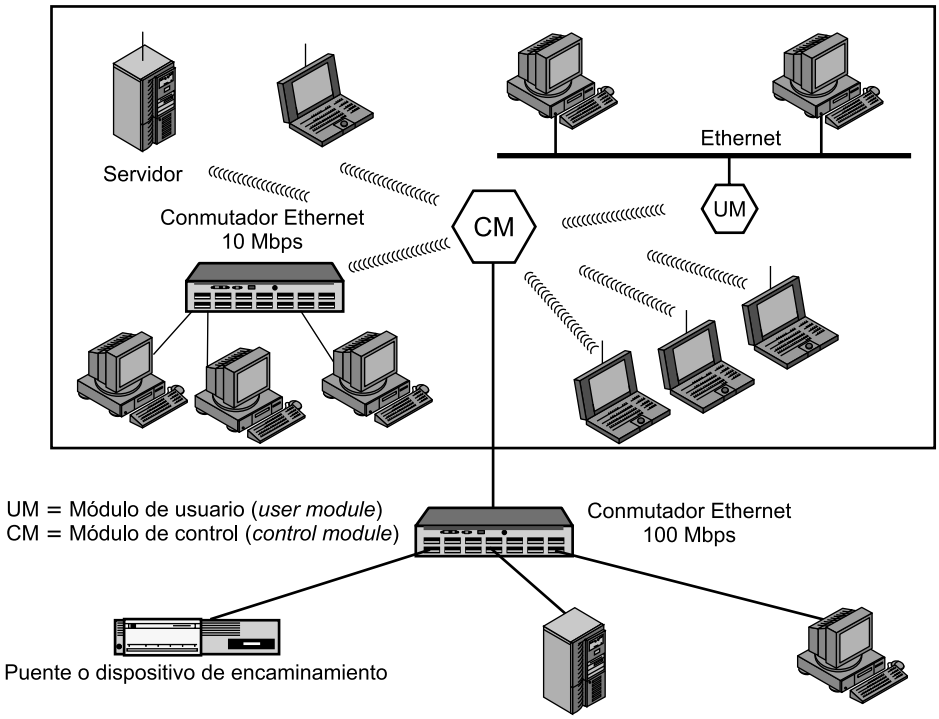


Figura 17.1. Ejemplo de configuración de una LAN inalámbrica de celda única.

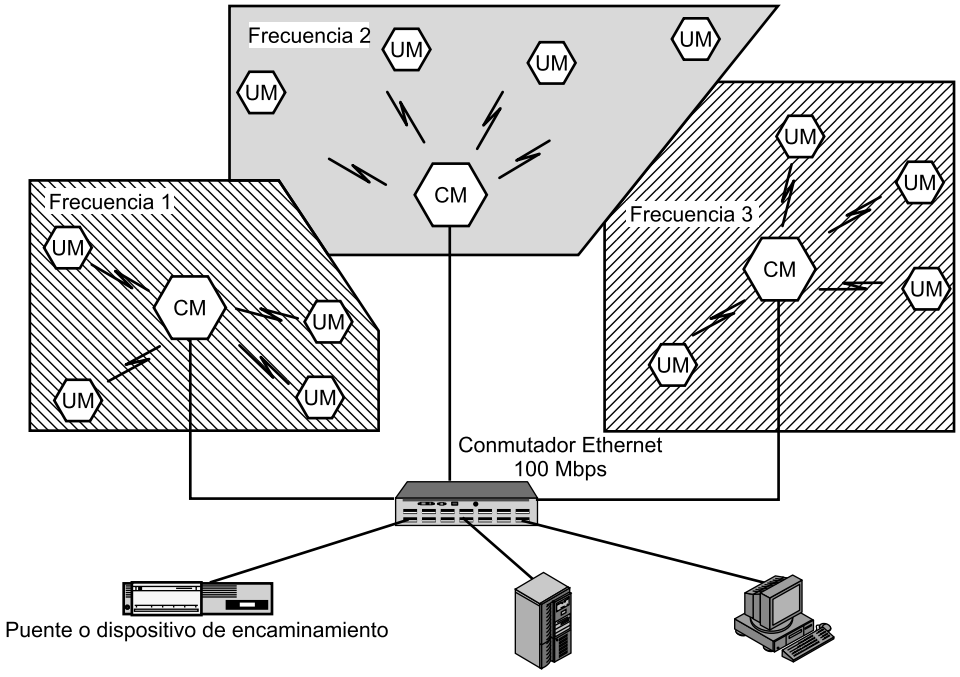


Figura 17.2. Ejemplo de configuración de una LAN inalámbrica de celdas múltiples.

Interconexión de edificios

Otra aplicación de las LAN de tecnología inalámbrica es la conexión de redes LAN situadas en edificios vecinos, sean LAN cableadas o inalámbricas. En este caso se usa un enlace punto a punto inalámbrico entre los dos edificios. Los dispositivos así conectados son, generalmente, puentes o dispositivos de encaminamiento. Este enlace punto a punto no es en sí mismo una LAN, pero es usual la inclusión de esta aplicación en el contexto de redes LAN inalámbricas.

Acceso nómada

El acceso nómada proporciona un enlace inalámbrico entre un concentrador de una LAN y un terminal de datos móvil equipado con una antena, como un computador portátil. Un ejemplo de la utilidad de este tipo de conexiones es posibilitar a un empleado que vuelve de un viaje la transferencia de datos desde un computador personal portátil a un servidor en la oficina. El acceso nómada resulta útil también en un entorno amplio, como un campus o un centro financiero situado lejos de un grupo de edificios. En ambos casos, los usuarios se pueden desplazar con sus computadores portátiles y pueden desear conectarse con los servidores de una LAN inalámbrica desde distintos lugares.

Trabajo en red *ad hoc*

Una red *ad hoc* es una red entre iguales (sin servidor central) establecida temporalmente para satisfacer alguna necesidad inmediata. Por ejemplo, un grupo de empleados, cada uno con su computador, puede reunirse para una cita de negocios o para una conferencia, conectando entre sí sus computadores en una red temporal sólo durante la reunión.

En la Figura 17.3 se sugieren las diferencias entre una LAN inalámbrica *ad hoc* y una LAN inalámbrica que proporciona ampliaciones de LAN y acceso nómada. En el segundo caso, la LAN inalámbrica presenta una infraestructura estacionaria consistente en una o más celdas con un módulo de control para cada una; dentro de cada celda pueden existir varios sistemas finales estacionarios. Las estaciones nómadas se pueden desplazar de una celda a otra. Por el contrario, en una red LAN *ad hoc* no existe infraestructura; más aún, un conjunto de estaciones localizadas en el mismo dominio se pueden autoconfigurar dinámicamente para formar una red temporalmente.

REQUISITOS DE LAS REDES LAN INALÁMBRICAS

Una LAN inalámbrica debe cumplir los mismos requisitos típicos de cualquier otra red LAN, incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad total entre las estaciones pertenecientes a la red y capacidad de difusión. Además de las mencionadas, existe un conjunto de necesidades específicas para entornos de LAN inalámbricas. Entre las más importantes se encuentran las siguientes:

- **Rendimiento:** el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio inalámbrico para maximizar la capacidad.
- **Número de nodos:** las LAN inalámbricas pueden necesitar dar soporte a cientos de nodos mediante el uso de varias celdas.
- **Conexión a la LAN troncal:** en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de LAN inalámbricas con in-

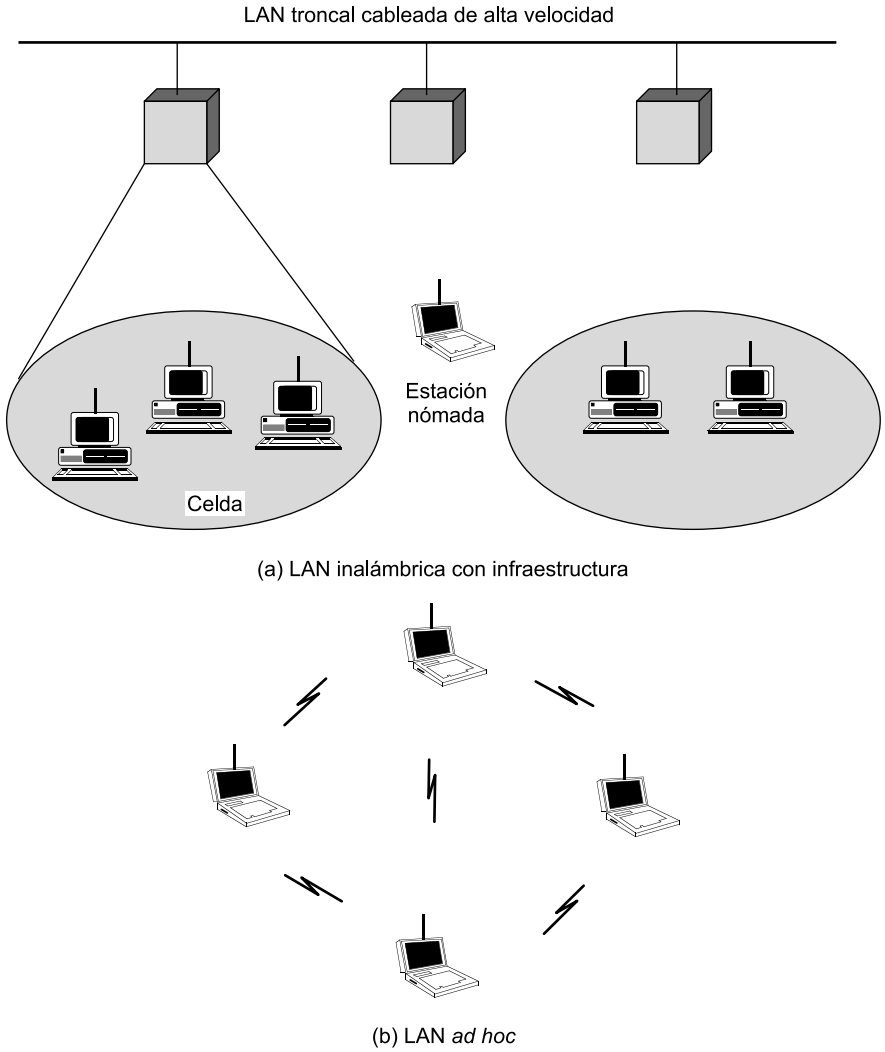


Figura 17.3. Configuraciones de redes LAN inalámbricas.

fraestructura, esto se consigue fácilmente a través del uso de módulos de control que conectan con ambos tipos de LAN. Puede ser también necesario dar soporte a usuarios móviles y redes inalámbricas *ad hoc*.

- **Área de servicio:** una zona de cobertura para una red LAN inalámbrica tiene un diámetro típico de entre 100 y 300 metros.
- **Consumo de energía:** los usuarios móviles utilizan estaciones de trabajo con batería que necesitan tener una larga vida cuando se usan con adaptadores sin cable. Esto sugiere que resulta inapropiado un protocolo MAC que requiera que los nodos móviles supervisen constantemente los puntos de acceso o realicen comunicaciones frecuentes con una estación base. Las implementaciones típicas de LAN inalámbricas poseen características propias para reducir el consumo de potencia mientras no se esté usando la red, como un modo de descanso (*sleep mode*).

- **Robustez en la transmisión y seguridad:** a menos que exista un diseño apropiado, una LAN inalámbrica puede ser propensa a sufrir interferencias y escuchas. El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.
- **Funcionamiento de redes adyacentes:** a medida que las LAN inalámbricas se están haciendo más populares, es probable que dos o más de estas redes operen en la misma zona o en alguna en la que sea posible la interferencia entre ellas. Estas interferencias pueden repercutir negativamente en el funcionamiento normal del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.
- **Funcionamiento sin licencia:** los usuarios preferirían adquirir y trabajar sobre LAN inalámbricas que no precisen de una licencia para la banda de frecuencias usada por la red.
- **Traspasos (*Handoff*)/Itinerancia (*Roaming*):** el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.
- **Configuración dinámica:** los aspectos de direccionamiento MAC y de gestión de la red LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

17.2. TECNOLOGÍA LAN INALÁMBRICA

Las redes LAN inalámbricas se clasifican, generalmente, de acuerdo con la técnica de transmisión usada. Todas las LAN inalámbricas actuales se encuentran dentro de una de las siguientes categorías:

- **LAN de infrarrojos (IR, *Infrared*):** una celda individual en una LAN IR está limitada a una sola habitación, dado que la luz infrarroja no es capaz de atravesar muros opacos.
- **LAN de espectro expandido:** este tipo de LAN hace uso de tecnologías de transmisión de espectro expandido. En la mayoría de los casos, estas LAN funcionan en las bandas ISM (industria, ciencia y medicina), de modo que no se necesita licencia FCC (*Federal Communications Comission*) para su utilización en los Estados Unidos.
- **Microondas de banda estrecha:** estas LAN operan en el rango de las microondas, pero no hacen uso de espectro expandido. Algunos de estos productos funcionan a frecuencias para las que es necesaria una licencia FCC, mientras que otras lo hacen en alguna de las bandas ISM.

En la Tabla 17.1 se resumen algunas de las principales características de estas tres tecnologías. A continuación, se proporcionan algunos detalles sobre ellas.

REDES LAN DE INFRARROJOS

Las comunicaciones ópticas inalámbricas en la banda infrarroja del espectro son de uso común en muchos hogares, estando presentes para el control remoto de numerosos dispositivos. Más recientemente, el interés se ha desplazado hacia el uso de la tecnología infrarroja para la construcción de redes LAN inalámbricas. Antes de comentar los detalles de esta tecnología, comenzaremos esta sección con una comparación entre las características de las LAN infrarrojas frente a aquellas que hacen uso de radio.

Tabla 17.1. Comparación de las tecnologías de redes LAN inalámbricas.

	Infrarrojos		Espectro expandido		Radio
	Infrarrojos difusos	**Infrarrojos de haz directo**	**Salto de frecuencia**	**Secuencia directa**	**Microondas de banda estrecha**
Velocidad (Mbps)	1-4	1-10	1-3	2-50	10-20
Movilidad	Estacionario/móvil	Estacionario con LOS	Móvil	Estacionario/móvil	
Alcance (m)	15-60	25	30-100	30-250	10-40
Detectabilidad	Despreciable		Pequeña		Alguna
Longitud de onda/frecuencia	λ: 800-900 nm		902-928 MHz 2,4-2,4835 GHz 5,725-5,85 GHz		902-928 MHz 5,2-5,775 GHz 18,825-19,205 GHz
Técnica de modulación	ASK		FSK	QPSK	FS/QPSK
Potencia radiada	—		$<$1 W		25 mW
Método de acceso	CSMA	Anillo con paso de testigo, CSMA	CSMA		Reserva, ALOHA, CSMA
Necesidad de licencia	No		No		Sí a menos que sea ISM

Ventajas y desventajas

Los dos medios de transmisión por excelencia para las LAN inalámbricas son las microondas de radio, usando espectro expandido o bien transmisión en banda estrecha, e infrarrojos. El uso de infrarrojos presenta una serie de ventajas significativas frente a los enfoques basados en microondas de radio. En primer lugar, el espectro de los infrarrojos es virtualmente ilimitado, lo que ofrece la posibilidad de alcanzar velocidades de datos extremadamente altas. El espectro de los infrarrojos no se encuentra regulado internacionalmente, cuestión ésta que no es cierta para algunas porciones del espectro de microondas.

Además de lo anterior, los infrarrojos comparten algunas propiedades con la luz visible que los hacen atractivos para su uso en ciertos tipos de configuraciones LAN. La luz infrarroja se refleja difusamente por los objetos de color, siendo así posible utilizar la reflexión producida en el techo para proporcionar cobertura a toda una habitación. El hecho de que la luz infrarroja no atraviese muros u otros objetos opacos presenta dos ventajas. En primer lugar, las comunicaciones infrarrojas pueden ser aseguradas contra escuchas de forma más sencilla que las de microondas. Por otro lado, en cada habitación de un edificio puede funcionar una instalación de infrarrojos aislada sin interferencias, posibilitando así la construcción de redes LAN infrarrojas muy grandes.

Otro hecho a favor de la tecnología de infrarrojos es que los equipos son relativamente baratos y simples. Generalmente, la transmisión por infrarrojos usa modulación en intensidad, de manera que los receptores IR únicamente necesitan detectar la amplitud de las señales ópticas. Por el contrario, la mayoría de los receptores de microondas precisan de la detección de la frecuencia o la fase.

El medio infrarrojo, por otro lado, exhibe asimismo algunas desventajas. Muchos entornos de interior sufren una radiación infrarroja de fondo debida tanto a la luz solar como a la artificial. Esta radiación ambiental, que se manifiesta en forma de ruido en el receptor, obliga a utilizar transmisores de alta potencia que limitan el alcance de la señal. Sin embargo, los incrementos en la potencia de la señal se han de limitar por dos factores: posibles daños a los ojos y consumo excesivo de potencia.

Técnicas de transmisión

Existen tres técnicas alternativas que se usan comúnmente para la transmisión IR de datos. La señal transmitida puede ser direccional (enfocada, como en el mando a distancia de la televisión), puede ser radiada omnidireccionalmente, o bien reflejada por el techo.

Un **haz IR dirigido** puede utilizarse para crear enlaces punto a punto. En este modo, el alcance depende de la potencia de emisión y el grado de enfoque. Un enlace de datos IR dirigido puede alcanzar distancias hasta de kilómetros. Aunque tales alcances no sean necesarios para la construcción de redes LAN inalámbricas localizadas en una habitación, un enlace de estas características puede utilizarse para la interconexión de edificios a través de puentes o dispositivos de encaminamiento entre los que haya una línea de visión.

Otro uso de enlaces IR punto a punto restringidos a una habitación es en la construcción de una red LAN de paso de testigo en anillo. Los transceptores IR se disponen de tal forma que los datos circulen alrededor de ellos en una configuración en anillo. Cada transceptor soporta una estación de trabajo o un concentrador de estaciones que efectúa las funciones de puente.

En la **configuración omnidireccional** existe una estación base aislada que se encuentra en la línea de visión del resto de estaciones que conforman la LAN. Generalmente, esta estación se ubica en el techo y actúa como un repetidor multipunto. El transmisor del techo difunde una señal omnidireccional que es recibida por el resto de transceptores IR en la zona. Por otro lado, cada transceptor emite un haz direccional apuntado hacia la unidad base localizada en el techo.

En una configuración de **difusión** todos los transmisores IR están enfocados hacia un punto en un techo reflectante. La radiación IR que alcanza el techo es reflejada omnidireccionalmente y recogida por todos los receptores en la zona.

REDES LAN DE ESPECTRO EXPANDIDO

Actualmente, las redes LAN inalámbricas más populares son aquellas que utilizan técnicas de espectro expandido.

Configuración

Exceptuando el caso de oficinas bastante reducidas, una LAN inalámbrica de espectro expandido hace uso de una disposición de celdas múltiples como la ilustrada en la Figura 17.2. Las celdas adyacentes utilizan diferentes frecuencias dentro de la misma banda para evitar interferencias.

Dentro de cada celda puede usarse una topología basada en un concentrador o bien una entre iguales (*peer to peer*). En una topología basada en un concentrador, como la indicada en la Figura 17.2, éste suele ubicarse en el techo y conectarse a una LAN cableada troncal para proporcionar conectividad entre las estaciones conectadas a las diversas redes locales (cableadas o

inalámbricas pertenecientes a otras celdas). El concentrador puede también controlar el acceso como en el caso de la función de coordinación puntual de 802.11, actuando como un repetidor multipunto, con una funcionalidad similar a la ofrecida por los repetidores multipunto Ethernet de 10 Mbps y 100 Mbps. En este caso, todas las estaciones en la celda transmiten únicamente hacia el concentrador y reciben exclusivamente de él. Alternativamente, y con independencia del mecanismo de control de acceso, cada estación puede difundir usando una antena omnidireccional, de tal forma que el resto de estaciones en la celda pueden recibir. Esto último se corresponde con una configuración lógica en bus.

Otra función potencial de un concentrador es el traspaso automático de las estaciones móviles. En cualquier instante, una serie de estaciones se encuentran asignadas a un concentrador dado de acuerdo con un criterio de proximidad. En el momento en que el concentrador percibe que una señal se debilita, puede traspasar la estación automáticamente al concentrador adyacente más próximo.

En una topología entre iguales no existe concentrador alguno, utilizándose algoritmos MAC como CSMA para controlar el acceso. Esta topología es apropiada para redes LAN *ad-hoc*.

Cuestiones de transmisión

Una característica deseable, aunque no necesaria, de una red LAN inalámbrica es que pueda ser utilizada sin requerir una licencia para la transmisión. Las regulaciones concernientes a las licencias difieren de un país a otro, lo que complica aún más este objetivo. En los Estados Unidos, la FCC ha autorizado dos aplicaciones dentro de la banda ISM que pueden operar sin licencia: sistemas basados en espectro expandido, que pueden funcionar hasta a 1 vatio, y sistemas de potencia reducida, que pueden funcionar hasta a 0,5 vatios. Dado que esta banda fue incorporada por la FCC, su uso para las redes LAN inalámbricas de espectro expandido se ha vuelto muy popular.

En los Estados Unidos se han reservado tres bandas de microondas para su uso sin licencia con espectro expandido: 902-928 MHz (banda de los 915 MHz), 2,4-2,4835 MHz (banda de los 2,4 GHz) y 5,725-5,825 GHz (banda de los 5,8 GHz). De todas ellas, la banda de los 2,4 GHz es utilizada también para este propósito en Europa y Japón. A medida que la frecuencia es más alta, el ancho de banda potencial es también mayor, de manera que las tres bandas anteriores se encuentran ordenadas por el atractivo que despiertan desde el punto de vista de la capacidad ofrecida. Por otra parte, se deben considerar las interferencias procedentes de otros dispositivos. Existen diversos dispositivos que funcionan alrededor de los 900 MHz, incluyendo teléfonos y micrófonos inalámbricos y radioaficionados. El número de dispositivos que operan en la banda de los 2,4 GHZ es más reducido. Un ejemplo notable son los hornos microondas, que tienden a sufrir mayores pérdidas de radiación con la edad. Actualmente, la competición en la banda de los 5,8 GHz es escasa. Sin embargo, nótese que, en términos generales, el coste de los equipos es mayor a medida que funcionan a frecuencias más elevadas.

REDES LAN DE MICROONDAS DE BANDA ESTRECHA

El término *microondas de banda estrecha* se refiere al uso de una banda de frecuencias de microondas de radio para la transmisión de la señal, siendo esta banda relativamente estrecha (el ancho suficiente para acomodar la señal). Hasta muy recientemente, todos los productos LAN basados en microondas de banda estrecha han utilizado una banda de microondas que requería licencia. Actualmente existe al menos un vendedor que ofrece un producto LAN en la banda ISM.

RF de banda estrecha con licencia

Las frecuencias de radio (RF) de microondas utilizables para la transmisión de voz, datos y vídeo se encuentras sujetas a licencias de uso y coordinadas dentro de cada zona geográfica para evitar posibles interferencias entre sistemas. Dentro de los Estados Unidos, las licencias se encuentran controladas por la FCC. Cada zona geográfica tiene un radio de 28 km y puede contener cinco licencias, cubriendo cada una de ellas dos frecuencias. Motorola posee 600 licencias (1.200 frecuencias) en el rango de los 18 GHz que cubre todas las áreas metropolitanas con población superior a los 30.000 habitantes.

Generalmente, un esquema de banda estrecha hace uso de una configuración en celdas como la ilustrada en la Figura 17.2. Las celdas adyacentes utilizan bandas de frecuencias no solapadas dentro de la banda global de los 18 GHz. En los Estados Unidos, puesto que Motorola controla la banda de frecuencias, se asegura que redes LAN independientes ubicadas en zonas geográficas próximas no interfieran entre sí. Las transmisiones son cifradas con objeto de proporcionar seguridad frente a escuchas.

Una ventaja de las LAN de banda estrecha con licencia es que garantizan una comunicación ausente de interferencias. Al contrario de lo que sucede con porciones del espectro no reguladas, como la banda ISM, la zona sujeta a licencias le proporciona un derecho legal al poseedor de la licencia de un canal de comunicaciones libre de interferencias. Los usuarios de una LAN en la banda ISM son susceptibles de sufrir interferencias en sus comunicaciones, careciendo de una solución legal para este problema.

RF de banda estrecha sin licencia

RadioLAN se convirtió en 1995 en el primer proveedor en presentar una red LAN inalámbrica de banda estrecha que utilizaba la zona ISM del espectro. Esta banda puede ser utilizada para transmisiones de banda estrecha a baja potencia (0,5 vatios o menos). El producto de RadioLAN funciona a 10 Mbps en la banda de los 5,8 GHz, alcanzando distancias de 50 m en una oficina semiabierta y de 100 m en una completamente abierta.

Este producto hace uso de una configuración entre iguales con una característica interesante. Como sustituto de un conmutador estacionario, el producto de RadioLAN elige automáticamente a un nodo como maestro dinámico, de acuerdo a parámetros como la localización, el nivel de interferencias y la potencia de la señal. La identidad del maestro puede cambiar dinámicamente a medida que las condiciones cambien. La red LAN incluye también una función de repetición dinámica que permite a cada estación actuar como un repetidor para mover datos entre estaciones que se encuentran entre sí fuera de la distancia máxima permitida.

17.3. ARQUITECTURA Y SERVICIOS DE IEEE 802.11

En 1990 se formó el comité IEEE 802.11 con el propósito de desarrollar un protocolo MAC y una especificación del medio físico para redes LAN inalámbricas. La Tabla 17.2 define brevemente los términos clave utilizados en el estándar IEEE 802.11.

ARQUITECTURA DE IEEE 802.11

En la Figura 17.4 se ilustra el modelo desarrollado por el grupo de trabajo IEEE 802.11. El componente elemental de una red LAN inalámbrica es un conjunto básico de servicios (BSS, *Basic*

Tabla 17.2. Terminología IEEE 802.11.

Punto de acceso (AP)	Cualquier entidad que tenga la funcionalidad de una estación y proporcione acceso al sistema de distribución a través del medio inalámbrico a las estaciones asociadas.
Conjunto básico de servicios (BSS)	Conjunto de estaciones controladas por una sola función de coordinación.
Función de coordinación	Función lógica que determina cuándo una estación funcionando dentro de un BSS tiene permiso para transmitir y puede recibir PDU.
Sistema de distribución (DS)	Sistema utilizado para interconectar un conjunto de BSS y LAN integradas para crear un ESS.
Conjunto extendido de servicios (ESS)	Conjunto de uno o más BSS interconectados y LAN integradas que aparece como un único BSS en la capa LLC de cualquier estación asociada con uno de tales BSS.
Unidad de datos del protocolo MAC (MPDU)	Unidad de datos intercambiada entre entidades MAC paritarias usando los servicios de la capa física.
Unidad de datos del servicio MAC (MSDU)	Información entregada como una unidad entre usuarios MAC
Estación	Cualquier dispositivo que contenga capas físicas y MAC compatibles con IEEE 802.11

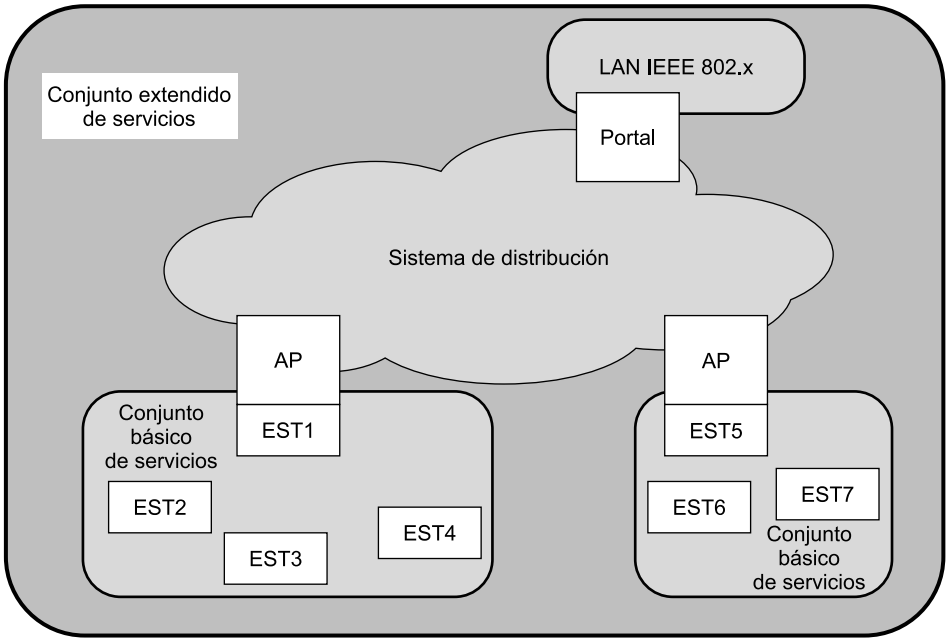


Figura 17.4. Arquitectura IEEE 802.11.

Service Set), consistente en un número de estaciones ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido. Un BSS puede funcionar aisladamente o bien estar conectado a un sistema troncal de distribución (DS, *Distribution System*) a

través de un punto de acceso (AP, *Access Point*) que efectúa las funciones de puente. El protocolo MAC puede ser completamente distribuido o bien estar controlado por una función central de coordinación ubicada en el punto de acceso. Generalmente, el BSS se corresponde con lo que en la bibliografía es referido como «celda». Por otro lado, el DS puede ser un conmutador, una red cableada tradicional u otra red inalámbrica.

La configuración más simple posible es la mostrada en la Figura 17.4, en la que cada estación pertenece a un BSS aislado; esto es, cada estación se encuentra dentro del rango de otras estaciones que pertenecen al mismo BSS. Es igualmente posible que exista un solapamiento geográfico entre dos BSS, de manera que una estación podría formar parte de más de un BSS. Además, la asociación entre una estación y un BSS es dinámica, puesto que una estación puede apagarse, salirse de la distancia máxima permitida o incorporarse de nuevo.

Un conjunto extendido de servicios (ESS, *Extended Service Set*) consiste en dos o más conjuntos básicos de servicios interconectados mediante un sistema de distribución. Este último es, por lo general, una LAN cableada troncal, aunque puede tratarse de cualquier red de comunicaciones. El conjunto extendido de servicios aparece a nivel de control de enlace lógico (LLC) como una única red LAN lógica.

En la Figura 17.4 se indica que un AP se implementa como parte de una estación. El AP constituye la lógica dentro de la estación que proporciona el acceso al DS a través de los servicios de distribución, además de servir como estación. La integración de una arquitectura 802.11 con una red LAN cableada tradicional se realiza a través de un portal. La lógica del portal se implementa en un elemento, como un puente o un dispositivo de encaminamiento, que forme parte de la LAN cableada y que se encuentre conectado al DS.

SERVICIOS DE IEEE 802.11

La normativa IEEE 802.11 define nueve servicios que deben ser proporcionados por una red inalámbrica para ofrecer una funcionalidad equivalente a la inherente a una LAN cableada tradicional. En la Tabla 17.3 se enumeran estos servicios y se indican dos formas de categorizarlos.

Tabla 17.3. Servicios de IEEE 802.11.

Servicio	Proveedor	Usado para dar soporte a
Asociación	Sistema de distribución	Entrega de MSDU
Autenticación	Estación	Acceso a la LAN y seguridad
Fin de la autenticación	Estación	Acceso a la LAN y seguridad
Disociación	Sistema de distribución	Entrega de MSDU
Distribución	Sistema de distribución	Entrega de MSDU
Integración	Sistema de distribución	Entrega de MSDU
Entrega de MSDU	Estación	Entrega de MSDU
Privacidad	Estación	Acceso a la LAN y seguridad
Reasociación	Sistema de distribución	Entrega de MSDU

1. El proveedor de servicios puede ser tanto la estación como el DS. Los servicios de la estación son implementados en cada estación IEEE 802.11, incluyendo la estación que constituye el AP. Los servicios de distribución son proporcionados entre BSS diferentes y deben ser implementados en un AP o en cualquier otro dispositivo de propósito específico conectado al sistema de distribución.
2. Tres de los servicios enumerados se emplean para controlar el acceso a una LAN IEEE 802.11 y para proporcionar confidencialidad. Los seis servicios restantes dan soporte a la entrega de unidades de datos de servicio MAC (MSDU, *MAC Service Data Units*) entre estaciones. Una MSDU es un bloque de datos que el usuario MAC le pasa a la capa MAC, generalmente en la forma de una PDU LLC. Si una MSDU es demasiado grande para ser transmitida en una sola trama MAC, puede ser fragmentada y transmitida en una serie de tramas. La fragmentación se discutirá en la Sección 17.4.

Siguiendo el documento IEEE 802.11, a continuación discutiremos los servicios de acuerdo con un orden que clarifica el funcionamiento de una red ESS IEEE 802.11. La **entrega de MSDU**, que constituye el servicio básico, ya ha sido mencionada.

Distribución de mensajes dentro de un DS

Los dos servicios implicados en la distribución de mensajes dentro de un DS son la distribución y la integración. La **distribución** es el servicio primario utilizado por las estaciones para intercambiar tramas MAC cuando la trama debe atravesar el DS para pasar de una estación en un BSS a otra estación en un BSS diferente. Por ejemplo, considerando la Figura 17.4, supongamos que una trama es transmitida desde la estación 2 (EST 2) hasta la estación 7 (EST 7). La trama se envía desde la estación EST 2 hasta la estación EST 1, que es el AP para este BSS. El AP entrega la trama a continuación al DS, que se encarga de encaminarla hasta el AP asociado con la estación EST 5 en el BSS de destino. La estación EST 5 recibe la trama y la retransmite a la estación EST 7. Las cuestiones acerca de cómo se transporta el mensaje a través del DS caen fuera del alcance del estándar IEEE 802.11.

Si las dos estaciones que establecen la comunicación se encuentran dentro del mismo BSS, entonces el servicio de distribución pasa, lógicamente, a través del AP de dicho BSS.

El servicio de **integración** permite la transferencia de datos entre una estación situada en una LAN IEEE 802.11 y otra estación en una LAN IEEE 802.x que se encuentre integrada con la primera. El término *integrada* hace referencia a una LAN cableada que esté físicamente conectada con el DS y cuyas estaciones puedan conectarse de forma lógica a una LAN IEEE 802.11 a través del servicio de integración. Este servicio es el encargado de llevar a cabo la traducción de direcciones y cualquier otra conversión lógica requerida para el intercambio de datos.

Servicios relacionados con la asociación

El principal objetivo de la capa MAC es la transferencia de MSDU entre entidades MAC. Esta tarea es desempeñada por el servicio de distribución. Para que este servicio pueda llevar a cabo sus funciones, necesita disponer de información acerca de las estaciones que se encuentran dentro del ESS. Esta información es la proporcionada por los servicios relacionados con la asociación. Antes de que el servicio de distribución pueda entregar o aceptar datos de una estación, ésta debe estar *asociada*. Antes de explorar la noción de asociación es necesario describir el concepto de movilidad. El estándar define tres tipos de transiciones basadas en la movilidad:

- **Sin transición:** una estación de este tipo es estacionaria o se desplaza únicamente dentro del rango de comunicación directa de las estaciones conectadas a un solo BSS.
- **Transición BSS:** se define como el desplazamiento de una estación desde un BSS hasta otro BSS de destino ubicado en el mismo ESS. En este caso, la entrega de datos a la estación necesita que la función de direccionamiento sea capaz de reconocer la nueva localización de la estación.
- **Transición ESS:** se define como el desplazamiento de una estación desde un BSS ubicado en un determinado ESS hasta otro BSS perteneciente a un ESS diferente del primero. Esta situación se soporta únicamente debido a que la estación tiene libertad para moverse. Sin embargo, el mantenimiento de conexiones de capas altas sustentadas sobre 802.11 no puede garantizarse. De hecho, es probable que se produzca una interrupción del servicio.

Para entregar un mensaje dentro de un DS, el servicio de distribución necesita conocer dónde se encuentra ubicada la estación de destino. Específicamente, el DS necesita conocer la identidad del AP al que el mensaje deberá ser entregado con objeto de que tal mensaje alcance la estación de destino. Para satisfacer este requisito, una estación debe mantener una asociación con el AP dentro de su BSS actual. Existen tres servicios vinculados con este requisito:

- **Asociación:** establece una asociación inicial entre una estación y un AP. La identidad y dirección de una estación deben conocerse antes de que la misma pueda transmitir o recibir tramas en una LAN inalámbrica. Para ello, una estación debe establecer una asociación con un AP perteneciente a un BSS particular. A partir de entonces, el AP puede comunicar esta información a otros AP dentro del ESS con objeto de facilitar el encaminamiento y la entrega de tramas.
- **Reasociación:** permite que una asociación previamente establecida sea transferida desde un AP hasta otro, haciendo así posible que una estación móvil pueda desplazarse desde un BSS hasta otro.
- **Disociación:** constituye una notificación, bien de una estación o bien por parte de un AP, de que una asociación existente deja de tener validez. Una estación debería proporcionar este aviso antes de abandonar un ESS o apagarse. No obstante, las funciones de gestión MAC incluyen mecanismos para protegerse frente a estaciones que desaparezcan sin emitir esta notificación.

Servicios de acceso y privacidad

Existen dos características de una LAN cableada que no son inherentes a una LAN inalámbrica:

1. Para poder transmitir sobre una LAN cableada, una estación debe estar físicamente conectada a la misma. Sin embargo, en el caso de una red inalámbrica, cualquier estación situada dentro de un rango similar al de otros dispositivos de la red puede transmitir. Existe, en cierto sentido, una forma de autenticación en el contexto de una red cableada: se precisa una acción positiva y presumiblemente observable para conectar una estación a una LAN cableada.
2. Análogamente, con objeto de recibir una transmisión desde una estación que forma parte de una LAN cableada, la estación receptora debe igualmente estar conectada al medio. Sin embargo, en el caso de una red inalámbrica cualquier estación dentro del rango apropiado puede recibir. De esta forma, una LAN cableada proporciona cierto grado de privacidad, limitando la recepción de datos únicamente a aquellas estaciones conectadas a la LAN.

El estándar IEEE 802.11 define tres servicios que proporcionan estas dos características a una LAN inalámbrica:

- **Autenticación:** es utilizada para que una estación pueda comunicar su identidad a otras estaciones. En una LAN cableada se asume, por lo general, que el acceso a una conexión física lleva aparejado la potestad para conectar a la LAN. Esta hipótesis no es válida en un entorno inalámbrico, en el que la conectividad se adquiere simplemente poseyendo una antena que se encuentre sintonizada adecuadamente. El servicio de autenticación es utilizado por las estaciones para establecer su identidad con otras con las que se desee comunicar. El estándar IEEE 802.11 da soporte a varios esquemas de autenticación y permite que la funcionalidad de los mismos pueda extenderse. El estándar no impone ningún esquema de autenticación concreto, que podría ir desde algún procedimiento relativamente inseguro hasta esquemas de cifrado de llave pública. Sin embargo, el estándar IEEE 802.11 precisa de una autenticación correcta y aceptada mutuamente antes de que una estación pueda establecer una asociación con un AP.
- **Fin de la autenticación:** este servicio es invocado siempre que se vaya a dar por finalizada una autenticación existente.
- **Privacidad:** se utiliza para asegurar que los contenidos de los mensajes no sean leídos por alguien diferente al receptor legítimo. El estándar incluye el uso opcional de mecanismos de cifrado para asegurar la privacidad.

17.4. CONTROL DE ACCESO AL MEDIO EN IEEE 802.11

La capa MAC de IEEE 802.11 cubre tres aspectos funcionales: la entrega fiable de datos, el control de acceso y la seguridad. En esta sección se examinan los dos primeros, puesto que el área de la seguridad cae fuera de los objetivos de este texto.

ENTREGA FIABLE DE DATOS

Al igual que cualquier otra red inalámbrica, una LAN inalámbrica que utilice las capas física y MAC especificadas en el estándar IEEE 802.11 está sujeta a una considerable falta de fiabilidad. El ruido, las interferencias y otros efectos de propagación repercuten en la pérdida de un número significativo de tramas. Incluso disponiendo de códigos correctores de errores, es posible que muchas tramas MAC no sean recibidas apropiadamente. Se puede hacer frente a esta situación con mecanismos que proporcionen fiabilidad en capas más altas, como TCP. Sin embargo, los contadores de tiempo utilizados para la retransmisión en capas superiores son, por lo general, del orden de segundos. Es, por tanto, más eficiente abordar el problema de los errores en el nivel MAC. Con esta finalidad, el estándar IEEE 802.11 incluye un protocolo de intercambio de tramas. Cuando una estación recibe una trama de datos de otra estación, devuelve una trama de confirmación (ACK) a la estación de origen. Este intercambio es tratado como una unidad atómica, sin ser interrumpido por una transmisión procedente de cualquier otra estación. Si la fuente no recibe la confirmación en un intervalo corto de tiempo, bien porque la trama de datos resultó dañada, o bien porque lo fue la trama ACK de retorno, la fuente retransmite la trama.

De esta forma, el mecanismo básico de transferencia de datos en IEEE 802.11 implica un intercambio de dos tramas. Para mejorar más aún la fiabilidad, es posible utilizar un intercambio de cuatro tramas. En este esquema, la fuente emite inicialmente una trama de solicitud para enviar

(RTS, *Request to Send*) hacia el destino. La estación de destino responde con una trama de permiso para enviar (CTS, *Clear to Send*). Tras recibir la trama CTS, la fuente emite la trama de datos y el destino responde con una confirmación (ACK). La trama RTS alerta a todas las estaciones que se encuentran dentro del rango de recepción de la fuente de que una transmisión está en curso. El resto de estaciones se abstiene de transmitir con objeto de evitar que se produzca una colisión entre dos tramas transmitidas al mismo tiempo. Análogamente, la trama CTS alerta a todas las estaciones que están en el rango de recepción del destino de que se va a producir un intercambio. Aunque la parte RTS/CTS del protocolo de intercambio es una función requerida de la capa MAC, es posible deshabilitarla.

CONTROL DE ACCESO

El grupo de trabajo 802.11 ha considerado dos tipos de propuestas para algoritmos MAC: protocolos de acceso distribuido, en los que, como en el caso de Ethernet, la decisión para transmitir se distribuye sobre todos los nodos usando un mecanismo de detección de portadora; y, por otro lado, protocolos de acceso centralizado, que implican una regulación de la transmisión por una autoridad central de toma de decisiones. Un protocolo de acceso distribuido tiene sentido en el caso de una red *ad hoc* de estaciones paritarias, aunque puede ser también interesante en otras configuraciones de LAN inalámbricas que trabajen principalmente con tráfico a ráfagas. Un protocolo de acceso centralizado es más natural para configuraciones en las que una serie de estaciones inalámbricas se encuentran interconectadas entre sí y con algún tipo de estación base que actúa como pasarela hacia una LAN troncal cableada. También es especialmente útil cuando parte de los datos tiene algún requisito de tiempo real o alta prioridad.

El resultado final en el caso de 802.11 es un algoritmo MAC denominado DFWMAC (*Distributed Foundation Wireless MAC*) que proporciona un mecanismo de control de acceso distribuido sobre el que se ubica un control centralizado opcional. En la Figura 17.5 se ilustra esta arquitectura. La subcapa MAC inferior es la función de coordinación distribuida (DCF, *Distributed Coordination Function*). La DCF utiliza un algoritmo de contención para proporcionar acceso a la totalidad del tráfico. El tráfico asíncrono ordinario hace uso directamente de la DCF. La función de coordinación puntual (PCF, *Point Coordination Function*) es un algoritmo MAC centralizado usado para ofrecer un servicio libre de contención. La PCF se ubica justo por encima de la DCF y utiliza las características de ésta para asegurar el acceso a sus usuarios. A continuación, se estudian estas dos subcapas.

Función de coordinación distribuida

La subcapa DCF hace uso de un sencillo algoritmo CSMA (*Carrier Sense Multiple Access*, acceso múltiple con detección de portadora). Una estación escucha el medio cuando dispone de una trama para transmitir. Si el medio está libre, la estación puede transmitir; en otro caso, la estación debe esperar antes de transmitir hasta que se complete la transmisión en curso. La DCF no incluye una función de detección de colisiones (es decir, CSMA/CD) porque ésta no resulta práctica en una red inalámbrica. El rango dinámico de las señales en el medio es muy elevado, de tal forma que una estación que desee transmitir no puede distinguir de manera efectiva entre una señal entrante muy débil, y el ruido más los efectos de su propia transmisión.

Para asegurar un funcionamiento adecuado y equitativo de este algoritmo, la DCF incluye un conjunto de retardos que se ordenan de acuerdo con un esquema de prioridades. Comenzaremos considerando un retardo simple denominado espacio entre tramas (IFS, *Interframe Space*).

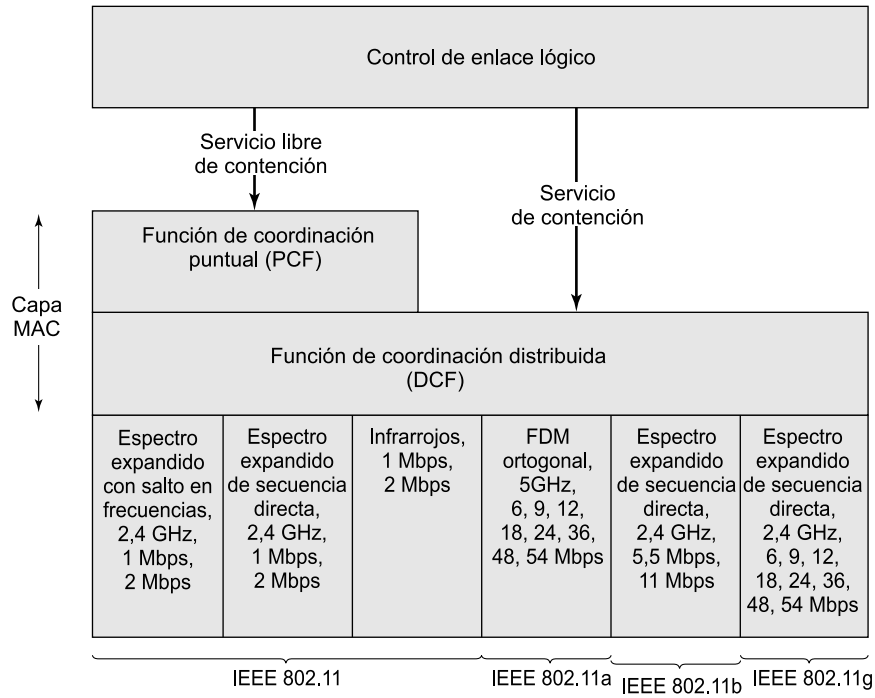

Control de enlace lógico
Servicio libre de contención
Servicio de contención
Función de coordinación puntual (PCF)
Capa MAC
Función de coordinación distribuida (DCF)
Espectro expandido con salto en frecuencias, 2,4 GHz, 1 Mbps, 2 Mbps
Espectro expandido de secuencia directa, 2,4 GHz, 1 Mbps, 2 Mbps
Infrarrojos, 1 Mbps, 2 Mbps
FDM ortogonal, 5GHz, 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Espectro expandido de secuencia directa, 2,4 GHz, 5,5 Mbps, 11 Mbps
Espectro expandido de secuencia directa, 2,4 GHz, 6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b
IEEE 802.11g

Figura 17.5. Arquitectura de protocolos IEEE 802.11.

De hecho, existen tres valores diferentes para el IFS, pero el algoritmo se explica mejor ignorando inicialmente este detalle. Usando un IFS, las reglas de acceso CSMA son las siguientes (*véase* la Figura 17.6):

1. Una estación que disponga de una trama lista para ser transmitida sondea el medio. Si éste se encuentra libre, la estación espera a ver si el medio permanece libre durante una cantidad de tiempo igual al IFS. Si es así, la estación puede transmitir inmediatamente.
2. Si el medio está ocupado (bien porque la estación lo encuentra inicialmente así, o bien porque este hecho sucede durante el tiempo de espera IFS), la estación pospone la transmisión y continúa monitorizando el medio hasta que la transmisión en curso finalice.
3. Una vez que la transmisión actual haya terminado, la estación espera otro IFS. Si el medio permanece libre durante ese periodo, la estación espera durante una cantidad aleatoria de tiempo y vuelve a sondear el medio de nuevo. Si el medio continúa libre, la estación puede transmitir. Si, por el contrario, el medio queda ocupado durante el periodo de espera, el contador de espera se para, comenzando de nuevo cuando el medio quede libre.

Para asegurar que el proceso de espera mantenga la estabilidad, se utiliza una espera exponencial binaria (descrita en el Capítulo 16), que proporciona una forma de manejar cargas elevadas. Los intentos repetidos y fallidos de transmitir se traducen en periodos de espera cada vez mayores, hecho éste que ayuda a reducir la carga. En el caso de que este mecanismo no existiera se podría dar la siguiente situación: dos o más estaciones intentan transmitir al mismo tiempo, ocasionando una colisión. Ambas intentan retransmitir inmediatamente, causando una nueva colisión.

El esquema anterior se refina para permitir que la DCF proporcione un acceso basado en prioridades. Para ello se utiliza un mecanismo simple basado en el uso de tres valores para el IFS:

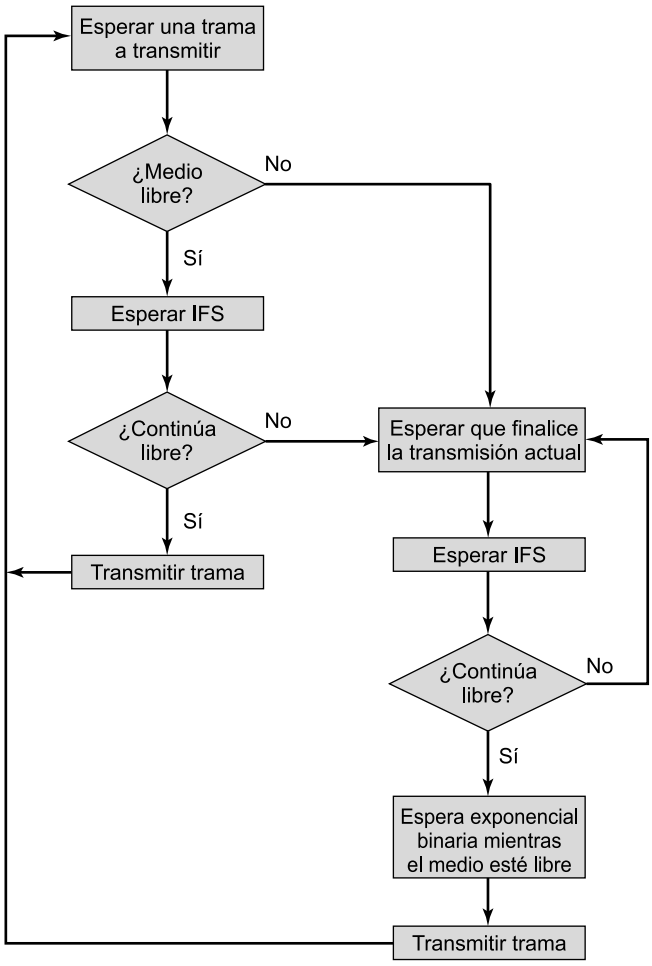


Figura 17.6. Lógica de control de acceso al medio en IEEE 802.11.

- **SIFS (IFS corto, *short IFS*):** es el IFS más pequeño y se utiliza para todas las acciones de respuesta inmediatas, tal y como se explica más adelante.
- **PIFS (IFS de la función de coordinación puntual, *Point coordination function IFS*):** se trata de un IFS de tamaño medio, utilizado por el controlador central en el esquema PCF cuando emite un sondeo.
- **DIFS (IFS de la función de coordinación distribuida, *Distributed coordination function IFS*):** constituye el IFS más grande y se usa como un retardo mínimo para las tramas asíncronas que compiten por el acceso al medio.

La Figura 17.7a ilustra el uso de estos valores de tiempo. Consideremos primeramente el caso del SIFS. Cualquier estación que utilice un SIFS para determinar la ocasión de transmitir tiene, en efecto, la prioridad más alta, dado que siempre ganará el acceso antes que cualquier otra estación que espere una cantidad de tiempo igual a un PIFS o a un DIFS. El uso de SIFS se produce en las siguientes circunstancias:

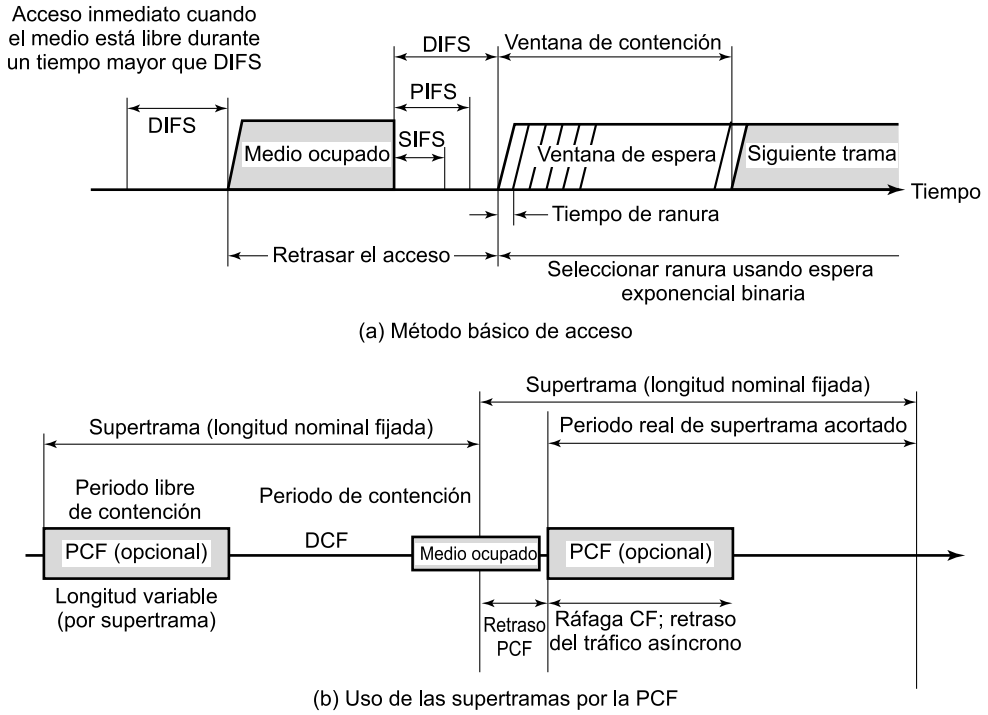


Figura 17.7. Ordenación temporal de los eventos MAC en IEEE 802.11.

- **Confirmación (ACK):** cuando una estación recibe una trama dirigida exclusivamente a ella (es decir, sin difusión ni multidifusión), ésta responde con una trama ACK tras esperar únicamente un espacio de tiempo igual a un SIFS. Esto tiene dos efectos deseables. En primer lugar, dado que no se utiliza detección de colisiones, la probabilidad de las colisiones es mayor que con CSMA/CD, de forma que la confirmación a nivel MAC proporciona un mecanismo eficiente de recuperación ante colisiones. En segundo lugar, el SIFS puede ser utilizado para proporcionar una entrega eficiente de una PDU correspondiente a un protocolo de nivel LLC que requiera varias tramas MAC. En este caso se da el siguiente escenario. Una estación con una PDU LLC multitrama lista para ser transmitida envía las tramas MAC una a una. Cada trama es confirmada tras un periodo de tiempo igual a un SIFS por el destinatario. Cuando la fuente recibe la confirmación (ACK), envía inmediatamente (tras un SIFS) la siguiente trama de la secuencia. El resultado es que, una vez que la estación ha competido por el canal, mantendrá el control sobre el mismo hasta que haya concluido el envío de todos los fragmentos de una PDU LLC.

- **Permiso para enviar (CTS):** una estación puede asegurar que su trama de datos se enviará satisfactoriamente si primero emite una pequeña trama de solicitud para enviar (RTS). La estación a quien va dirigida la trama RTS debería responder inmediatamente con una trama CTS si se encuentra preparada para recibir. El resto de estaciones reciben la trama RTS y se abstienen de usar el medio.

- **Respuesta a sondeo (*poll response*):** este punto es explicado posteriormente en la discusión sobre PCF.

El siguiente intervalo IFS en longitud es el PIFS. Éste es utilizado por el controlador central para la emisión de sondeos y tiene prioridad sobre el tráfico de contención normal. Obsérvese, sin embargo, que las tramas transmitidas utilizando SIFS tienen prioridad sobre un sondeo PCF.

Finalmente, el intervalo DIFS se utiliza para el tráfico ordinario asíncrono.

Función de coordinación puntual

PCF es un método de acceso alternativo implementado sobre DCF, cuya función consiste en un sondeo realizado por un elemento central de sondeos (coordinador puntual). El coordinador puntual hace uso de un PIFS cuando emite un sondeo. Dado que un PIFS es más pequeño que un DIFS, el coordinador puntual puede adueñarse del medio y bloquear todo el tráfico asíncrono mientras emite un sondeo y recibe las respuestas.

Como caso extremo puede considerarse el siguiente escenario posible. Una red inalámbrica se configura de tal manera que una serie de estaciones con tráfico sensible a los retardos se controla por medio del coordinador puntual, mientras que el resto del tráfico compite por el acceso usando CSMA. El coordinador puntual podría emitir consultas a todas las estaciones configuradas para el sondeo siguiendo un esquema de turno rotatorio. Cuando se emite un sondeo, la estación consultada puede responder utilizando un SIFS. Si el coordinador puntual recibe una respuesta, entonces emite un nuevo sondeo usando un PIFS. Si no se recibe respuesta alguna durante el tiempo correspondiente al turno, el coordinador emite un sondeo.

Si la disciplina expuesta en el párrafo anterior fuese implementada, el coordinador puntual podría bloquear todo el tráfico asíncrono sin más que emitir repetidamente sondeos. Para prevenir la ocurrencia de este hecho se define un intervalo conocido como supertrama. Durante la primera parte de este intervalo, el coordinador puntual emite sondeos a todas las estaciones configuradas para el sondeo siguiendo un esquema de turno rotatorio. A continuación, el coordinador espera un tiempo igual a lo que reste de la supertrama, permitiendo así la existencia de un periodo de contención para el acceso asíncrono.

En la Figura 17.7b se ilustra el uso de la supertrama. Al principio de una supertrama, el coordinador puntual puede hacerse con el control opcionalmente y emitir sondeos durante un periodo de tiempo dado. Este intervalo varía debido al tamaño variable que pueden tener las tramas de respuesta de las estaciones. El tiempo restante de la supertrama queda disponible para el acceso competitivo. Al final del intervalo de supertrama, el coordinador puntual compite por el acceso al medio usando un PIFS. Si el medio se encuentra disponible, el coordinador gana el acceso inmediatamente, siguiendo a continuación una supertrama completa. Sin embargo, el medio puede estar ocupado al final de la supertrama. En este caso, el coordinador puntual debe esperar hasta que el medio quede libre para conseguir el acceso, lo que se traducirá en un periodo de supertrama más corto para el siguiente ciclo.

TRAMA MAC

En la Figura 17.8 se muestra el formato de una trama 802.11. Este formato general se utiliza para todas las tramas de datos y de control, aunque no todos los campos se utilizan en todos los contextos. Los campos son los siguientes:

- **Control de trama:** indica el tipo de trama (control, gestión o datos) y proporciona información de control. La información de control indica si la trama proviene o va destinada a un DS, y contiene información de control y relativa a la privacidad.

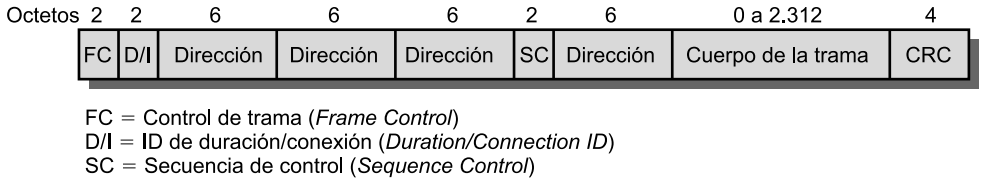


Figura 17.8. Formato de la trama MAC en IEEE 802.11.

- **ID de duración/conexión:** si se utiliza como un campo de duración, indica el tiempo (en microsegundos) que el canal será reservado para una transmisión satisfactoria de una trama MAC. En algunas tramas de control, este campo contiene el identificador de una asociación o de una conexión.
- **Direcciones:** el número y significado de los campos de direcciones dependen del contexto. Los tipos de direcciones son la de la fuente, el destino, la estación transmisora y la estación receptora.
- **Control de secuencia:** contiene un subcampo de 4 bits (número de fragmento) utilizado para la fragmentación y el reensamblado, y un número de secuencia de 12 bits utilizado para numerar las tramas enviadas entre un transmisor dado y un receptor.
- **Cuerpo de la trama:** contiene una MSDU completa o un fragmento de la misma. La MSDU es una unidad de datos del protocolo LLC o información de control MAC.
- **Secuencia de comprobación de trama:** se trata de una comprobación de redundancia cíclica de 32 bits.

A continuación, examinaremos los tres tipos de tramas MAC.

Tramas de control

Las tramas de control prestan servicio a la entrega fiable de tramas de datos. Existen seis subtipos de tramas de control:

- **Sondeo de ahorro de energía (PS-Poll, *Power Save-Poll*):** esta trama es enviada por cualquier estación hacia la estación que contiene el punto de acceso (AP). Su objetivo es solicitar al AP que transmita una trama destinada a esta estación que ha sido almacenada en una memoria temporal debido a que la estación se encontraba en modo de ahorro de energía.
- **Solicitud para enviar (RTS):** se trata de la primera trama en el protocolo de cuatro pasos discutido cuando se trató la entrega fiable de datos al principio de la Sección 17.3. La estación que envía este mensaje está alertando a un posible destino, así como al resto de las estaciones dentro del rango de recepción, de que pretende enviar una trama de datos a dicho destino.
- **Permiso para enviar (CTS):** se trata de la segunda trama en el protocolo de cuatro pasos. Es enviada por la estación de destino hacia la fuente para concederle permiso para emitir una trama de datos.
- **Confirmación:** proporciona una confirmación del destino hacia la fuente, indicando que los datos, información de gestión o sondeo de ahorro de energía previos han sido recibidos correctamente.

- **Fin de periodo libre de contención:** anuncia el final de un periodo libre de contenciones que forma parte de la función de coordinación puntual.
- **CF-End + CF-Ack:** confirmación de la trama CF-End. Esta trama finaliza el periodo libre de contención y libera a las estaciones de las restricciones asociadas con este periodo.

Tramas de datos

Existen ocho subtipos de tramas de datos, organizados en dos grupos. Los primeros cuatro subtipos definen tramas que transportan datos de una capa superior desde la estación origen hasta la estación de destino. Las cuatro tramas de transporte de datos son las siguientes:

- **Datos:** se trata de la trama de datos más simple. Puede ser utilizada tanto en el periodo de contención como en el periodo libre de contención.
- **Datos + CF-Ack:** únicamente puede ser enviada durante el periodo libre de contención. Además de transportar datos, esta trama confirma la recepción de otros previamente recibidos.
- **Datos + CF-Poll:** se utiliza por parte de un coordinador puntual para entregar datos a una estación móvil y para solicitar que ésta envíe una trama de datos que puede haber sido almacenada temporalmente.
- **Datos + CF-Ack + CF-Poll:** combina en una sola trama las funciones de las tramas Datos + CF-Ack y Datos + CF-Poll.

Los cuatro subtipos restantes de tramas de datos no transportan, en realidad, datos del usuario. La trama conocida como función nula (*Null Function*) no transporta datos, sondeos o confirmaciones. Se utiliza para transportar el bit de gestión de energía en el campo de control de una trama destinada al AP, indicando así que la estación va a entrar en un estado de operación de baja energía. Las tres tramas restantes (CF-Ack, CF-Poll y CF-Ack + CF-Poll) poseen la misma funcionalidad que los subtipos de tramas de datos correspondientes que se han comentado en la lista anterior (Datos + CF-Ack, Datos + CF-Poll, Datos + CF-Ack + CF-Poll), pero sin transportar datos.

Tramas de gestión

Las tramas de gestión se utilizan para gestionar las comunicaciones entre las estaciones y los puntos de acceso. Las funciones que cubren incluyen la gestión de las asociaciones (solicitud, respuesta, reasociación, disociación y autenticación).

17.5. CAPA FÍSICA DE IEEE 802.11

La capa física del estándar IEEE 802.11 ha sido definida en cuatro etapas. La primera parte fue publicada en 1997. Dos partes adicionales se publicaron en 1999 y, finalmente, la más reciente apareció en 2002. La primera de ellas, llamada simplemente IEEE 802.11, incluye la capa MAC y tres especificaciones de la capa física, dos en la banda de los 2,4 GHz y una en los infrarrojos, todas ellas operando a 1 y 2 Mbps. IEEE 802.11a funciona en la banda de los 5 GHz a velocidades de datos de hasta 54 Mbps. IEEE 802.11b funciona en la banda de los 2,4 GHz a 5,5 y 11 Mbps. IEEE 802.11g amplía la norma IEEE 802.11b a velocidades de datos más altas. A continuación, se examinan sucesivamente cada una de ellas.

CAPA FÍSICA ORIGINAL DE IEEE 802.11

En el estándar original 802.11 se definen tres medios físicos:

- Espectro expandido de secuencia directa (DS-SS) funcionando en la banda ISM de los 2,4 GHz, con velocidades de datos de 1 Mbps y 2 Mbps.
- Espectro expandido con salto en frecuencias (FH-SS) funcionando en la banda ISM de los 2,4 GHz, con velocidades de datos de 1 Mbps y 2 Mbps.
- Infrarrojos a 1 Mbps y 2 Mbps funcionando con longitudes de onda entre 850 nm y 950 nm.

Espectro expandido en secuencia directa

En el sistema DS-SS pueden utilizarse hasta siete canales, cada uno con una velocidad de datos de 1 Mbps o 2 Mbps. El número de canales disponible depende del ancho de banda reservado por las diversas agencias reguladoras. Éste puede variar desde los 13 disponibles en la mayoría de los países europeos hasta solamente 1 disponible en Japón. Cada canal tiene un ancho de banda de 5 MHz. El esquema de codificación utilizado es DBPSK para velocidades de 1 Mbps y DQPSK para el caso de 2 Mbps.

Espectro expandido con salto de frecuencias

Recordemos del Capítulo 7 que un sistema FH-SS hace uso de varios canales, saltando la señal de un canal a otro de acuerdo con una secuencia pseudoaleatoria. En el caso del esquema IEEE 802.11, se utilizan canales de 1 MHz. El número de canales disponibles varía desde 23 en Japón hasta 70 en los Estados Unidos.

Los detalles del esquema de saltos son ajustables. Por ejemplo, la tasa mínima de saltos en los Estados Unidos es de 2,5 saltos por segundo. La distancia mínima de cada salto en frecuencia es de 6 MHz en Norteamérica y la mayor parte de Europa, mientras que en Japón es de 5 MHz.

Para la modulación, el esquema FH-SS utiliza GFSK de dos niveles para el sistema a 1 Mbps. Los bits cero y uno se codifican como desviaciones de la frecuencia portadora actual. Para el sistema a 2 Mbps se utiliza un esquema GFSK de cuatro niveles en el que las cuatro combinaciones de 2 bits se definen mediante cuatro desviaciones diferentes de la frecuencia central.

Infrarrojos

El esquema de infrarrojos en IEEE 802.11 es omnidireccional en lugar de punto a punto, siendo posible cubrir distancias de hasta 20 m. El esquema de modulación para velocidades de datos de 1 Mbps se conoce como PPM-16 (*Pulse Position Modulation*). En este esquema, cada grupo de 4 bits de datos se transforma en uno de los 16 símbolos PPM, siendo cada símbolo una cadena de 16 bits. Cada cadena de 16 bits consta de quince ceros y un uno binario. En el caso de 2 Mbps, cada grupo de 2 bits se transforma en una de cuatro posibles secuencias de 4 bits. Cada secuencia consta de tres ceros y un uno binario. La transmisión real emplea un esquema de modulación en intensidad en el que la presencia de señal se corresponde con un 1 binario y la ausencia de la misma con un 0 binario.

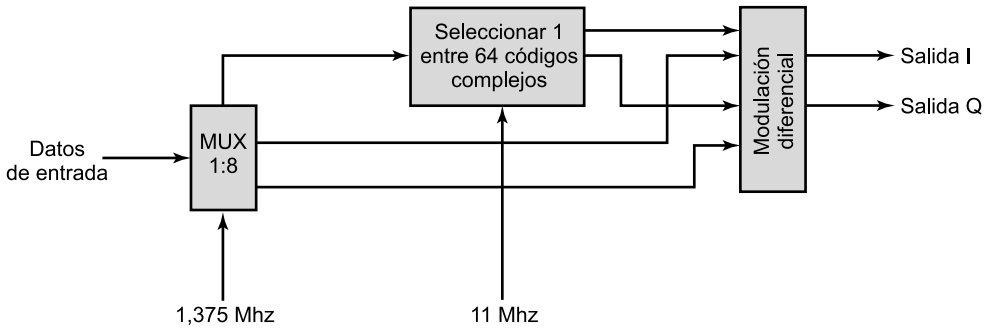


Figura 17.9. Esquema de modulación CCK a 11 Mbps.

IEEE 802.11a

La especificación IEEE 802.11a hace uso de la banda de los 5 GHz. Al contrario que en el caso de las especificaciones en la banda de los 2,4 GHZ, en IEEE 802.11a no se emplea un esquema de espectro expandido, sino multiplexación por división de frecuencia ortogonal (OFDM, *Orthogonal Frequency Division Multiplexing*). OFDM, también conocido como modulación multiportadora, utiliza varias señales portadoras con frecuencias diferentes, enviando algunos de los bits totales por cada canal. Se trata de un esquema similar a FDM. Sin embargo, en el caso de OFDM todos los subcanales están dedicados a una única fuente de datos.

Las velocidades de datos posibles en IEEE 802.11a son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. El sistema utiliza hasta 52 subportadoras que se modulan usando BPSK, QPSK, QAM-16 o QAM-64, en función de la velocidad requerida. El espaciado entre frecuencias subportadoras es de 0,3125 MHz. Un código convolucional a una tasa de 1/2, 2/3 o 3/4 proporciona corrección de errores hacia delante.

IEEE 802.11b

IEEE 802.11b es una extensión del esquema IEEE 802.11 DS-SS, proporcionando velocidades de datos de 5,5 y 11 Mbps. La tasa de minibits es de 11 MHz, la misma que el esquema DS-SS original, proporcionando así el mismo ancho de banda ocupado. Para conseguir una velocidad de datos mayor en el mismo ancho de banda y con la misma tasa de minibits se utiliza un esquema de modulación conocido como modulación por código complementario (CCK, *Complementary Code Keying*).

El esquema de modulación CCK es bastante complejo y no será examinado aquí en detalle. La Figura 17.9 proporciona una idea general del esquema para una velocidad de datos de 11 Mbps. Los datos de entrada son manejados en bloques de 8 bits a una tasa de 1,375 MHz (8 bits/símbolo $\times$ 1,375 MHz = 11 Mbps). Seis de estos bits son transformados en una de las 64 secuencias de código. La salida de esta transformación, junto con los dos bits adicionales, constituye la entrada de un modulador QPSK.

IEEE 802.11g

IEEE 802.11g es una extensión de IEEE 802.11b a mayor velocidad. Este esquema combina toda una gama de técnicas de codificación del medio físico utilizadas en 802.11a y 802.11b para proporcionar servicio a diversas velocidades de datos.

17.6. LECTURAS Y SITIOS WEB RECOMENDADOS

[PAHL95] y [BANT95] son artículos que examinan detalladamente las LAN inalámbricas. [KAHN97] es una buena referencia de las redes LAN de infrarrojos.

[OHAR99] contiene un excelente tratamiento técnico de IEEE 802.11. Otra buena referencia en este sentido es [LARO02]. [GEIE99] proporciona también un tratamiento detallado de los estándares IEEE 802.11 y numerosos casos de estudio. [CROW97] es un buen artículo de evaluación de los estándares 802.11. Ninguna de las dos últimas referencias cubre IEEE 802.11a y 802.11b. [GEIE01] incluye una buena explicación de IEEE 802.11a. [SHOE02] proporciona una visión general de IEEE 802.11b.

BANT94 Bantz, D., y Bauchot, F. «Wireless LAN Design Alternatives.» *IEEE Network*, marzo/abril 1994.

CROW97 Crow, B. *et al*., «IEEE 802.11 Wireless Local Area Networks.» *IEEE Communications Magazine*, septiembre 1997.

GEIE99 Geier, J. *Wireless LANs*. New York: Macmillan Technical Publishing, 1999.

GEIE01 Geier, J. «Enabling Fast Wireless Networks with OFDM.» *Communications System Design*, febrero 2001. (www.csdmag.com)

KAHN97 Kahn, J., y Barry, J. «Wireless Infared Communications.» *Proceedings of the IEEE*, febrero 1997.

LARO02 LaRocca, J., y LaRocca, R. *802.11 Demystified.* New York: McGraw-Hill, 2002.

OHAR99 Ohara, B., y Petrick, A. *IEEE 802.11 Handbook: A Designer's Companion.* New York: IEEE Press, 1999.

PAHL95 Pahlavan, K.; Probert, T., y Chase, M. «Trends in Local Wireless Networks.» *IEEE Communications Magazine*, marzo 1995.

SHOE02 Shoemake, M. «IEEE 802.11g Jells as Applications Mount.» *Communications System Design*, abril 2002.www.commsdesign.com.

SITIOS WEB RECOMENDADOS

- **Asociación de LAN Inalámbricas (*Wireless LAN Alliance*):** proporciona una introducción a la tecnología, incluyendo una discusión sobre consideraciones de implementación y casos de estudio particulares de usuarios. Contiene enlaces a sitios relacionados.
- **Grupo de Trabajo de LAN Inalámbricas IEEE 802.11 (*The IEEE 802.11 Wireless LAN Working Group*):** contiene los documentos del grupo de trabajo y archivos sobre las discusiones.
- **Alianza Wi-Fi (*Wi-Fi Alliance*):** grupo de industrias que promociona la interoperabilidad entre productos 802.11 y entre éstos con Ethernet.

17.7. TÉRMINOS CLAVE Y CUESTIONES DE REPASO

TÉRMINOS CLAVE

acceso nómada
conjunto básico de servicios (BSS)
conjunto extendido de servicios (ESS)
extensión de redes LAN
función de coordinación
función de coordinación distribuida (DCF)
función de coordinación puntual (PCF)
funcionamiento en redes *ad-hoc*
LAN de espectro expandido
LAN inalámbrica
LAN de infrarrojos
LAN de microondas de banda estrecha
modulación por código complementario (CCK)
punto de acceso (AP)
secuencia de Barker
sistema de distribución (DS)

CUESTIONES DE REPASO

17.1. Enumere y defina brevemente cuatro áreas de aplicación para las LAN inalámbricas.

17.2. Enumere y defina brevemente los requisitos clave para las LAN inalámbricas.

17.3. ¿Qué diferencia existe entre una LAN inalámbrica de celda única y una de celdas múltiples?

17.4. Enumere algunas de las principales ventajas de las LAN de infrarrojos.

17.5. Enumere algunas de las principales desventajas de las LAN de infrarrojos.

17.6. Enumere y defina brevemente tres técnicas de transmisión utilizadas en LAN de infrarrojos.

17.7. ¿Qué diferencia hay entre un punto de acceso y un portal?

17.8. ¿Un sistema de distribución es una red inalámbrica?

17.9. Enumere y defina brevemente los servicios de IEEE 802.11.

17.10. ¿Cómo se relaciona el concepto de asociación con el de movilidad?

PARTE V

PROTOCOLOS DE INTERCONEXIÓN

CUESTIONES DE LA PARTE V

Hasta ahora hemos tratado con tecnologías y técnicas utilizadas para intercambiar datos entre dos dispositivos. La Parte II trataba el caso en el que los dos dispositivos comparten un enlace de transmisión. Las Partes III y IV estaban relacionadas con el caso en el que una red de comunicación proporciona una capacidad de transmisión compartida entre múltiples sistemas finales conectados.

En un sistema de procesamiento de datos distribuido se necesita mucho más. Los sistemas de procesamiento de datos (estaciones de trabajo, PC, servidores y grandes computadores) deben implementar un conjunto de funciones que les permitirán llevar a cabo algunas tareas de forma cooperativa. Este conjunto de funciones se organiza en una arquitectura de comunicaciones e implica la utilización de un conjunto de protocolos en capas, incluyendo protocolos de interconexión, de transporte y de la capa de aplicación.

Antes de proceder con la Parte V, se aconseja al lector que revise el Capítulo 2, que introduce el concepto de arquitectura de protocolos y discute los elementos clave de un protocolo.

ESQUEMA DE LA PARTE V

CAPÍTULO 18. PROTOCOLOS DE INTERCONEXIÓN DE REDES

Con la proliferación de las redes, los equipos de interconexión han llegado a ser componentes esenciales del diseño de red. El Capítulo 18 comienza examinando las necesidades de un equipo de interconexión y los diversos enfoques de diseño que se pueden tomar para satisfacer estas necesidades. El resto del capítulo trata la utilización de los dispositivos de encaminamiento para la interconexión. Se examina el protocolo de Internet (IP) y el nuevo IPv6.

CAPÍTULO 19. FUNCIONAMIENTO DE LA INTERCONEXIÓN DE REDES

El Capítulo 19 comienza discutiendo la multidifusión a través de una internet. A continuación se exponen las cuestiones relacionadas con el encaminamiento y la calidad de servicio.

El tráfico que Internet y las redes privadas deben transportar lleva a un crecimiento y cambio continuos. La demanda generada por las aplicaciones tradicionales basadas en datos, como el correo electrónico, los grupos de noticias Usenet, la transferencia de ficheros y la conexión remota, es todo un reto para el desarrollo de estos sistemas. Pero el factor impulsor es la extraordinaria carga que supone la WWW (World Wide Web), que demanda respuestas en tiempo real, y el uso creciente de la voz, imágenes e incluso vídeo a través de arquitecturas de interconexión de redes.

Estos esquemas de interconexión están basados esencialmente en tecnologías de conmutación de paquetes por datagramas con dispositivos de encaminamiento funcionando como conmutadores. Estas tecnologías no se diseñaron para tratar voz o vídeo y se están adaptando para satisfacer las demandas que se le imponen. Aunque muchos prevén el reemplazo de este conglomerado de LAN basadas en Ethernet, WAN basadas en paquetes y dispositivos de encaminamiento basados en datagramas IP por un servicio de transporte ATM sin fisuras desde el puesto de trabajo hasta la red central, ese día parece lejano. Mientras tanto, la función de interconexión y de encaminamiento de estas redes debe de adecuarse para satisfacer las necesidades crecientes de esta carga.

El Capítulo 19 examina algunas de las herramientas y técnicas diseñadas para satisfacer las nuevas demandas, empezando con una discusión sobre las técnicas de encaminamiento, que pueden ayudar a suavizar una carga repentina imprevista. El resto del capítulo analiza los esfuerzos recientes para proporcionar un nivel dado de calidad de servicio (QoS) a varias aplicaciones. Los elementos más importantes de este nuevo enfoque son los servicios integrados y los servicios diferenciados.

CAPÍTULO 20. PROTOCOLOS DE TRANSPORTE

El protocolo de transporte es la piedra angular del concepto global de una arquitectura de comunicaciones de computadores. También puede ser uno de los protocolos más complejos. El Capítulo 20 examina en detalle los mecanismos del protocolo de transporte y luego discute dos ejemplos importantes, TCP y UDP. La mayor parte del capítulo está dedicada a un análisis del conjunto complejo de mecanismos de TCP y a los esquemas de control de congestión en TCP.

CAPÍTULO 21. SEGURIDAD EN REDES

La seguridad en red ha llegado a ser cada vez más importante con el crecimiento del número e importancia de las redes. El Capítulo 21 proporciona una visión general de las técnicas y servicios de seguridad. El capítulo comienza con una visión global a las técnicas de cifrado para asegurar la confidencialidad, que incluye la utilización del cifrado convencional y de clave pública. A continuación se explora el área de la autentificación y de las firmas digitales. Se examinan los dos algoritmos más importantes de cifrado, AES y RSA, así como SHA-1, una función mezcla de un solo sentido importante para un determinado número de aplicaciones de seguridad. Finalmente, el capítulo describe también SSL y el conjunto de estándares de seguridad en IP.

CAPÍTULO 22. APLICACIONES DISTRIBUIDAS

El propósito de una arquitectura de comunicaciones es dar soporte a aplicaciones distribuidas. En el Capítulo 22 se examinan tres de las más importantes de estas aplicaciones; en cada caso se discuten los principios generales, seguido de un ejemplo específico. Las aplicaciones distribuidas son el correo electrónico, los intercambios de la WWW y la gestión de red. Los ejemplos correspondientes son SMTP y MIME, HTTP y SNMP.

CAPÍTULO 18

Protocolos de interconexión de redes

18.1. Funciones básicas de los protocolos
Encapsulamiento
Fragmentación y reensamblado
Control de conexión
Entrega ordenada
Control de flujo
Control de errores
Direccionamiento
Multiplexación
Servicios de transmisión

18.2. Principios de la interconexión entre redes
Requisitos
Enfoques sobre la arquitectura

18.3. Interconexión entre redes sin conexión
Funcionamiento de un esquema de interconexión no orientado a conexión
Cuestiones de diseño

18.4. El protocolo Internet
Servicios IP
Protocolo IP
Direcciones IP
Protocolo de mensajes de control de internet (ICMP)

18.5. IPv6
IP de nueva generación
Estructura IPv6
Cabecera IPv6
Direcciones IPv6
Cabecera de opciones salto a salto
Cabecera de fragmentación
Cabecera de encaminamiento
Cabecera de opciones para el destino

18.6. Lecturas y sitios web recomendados

18.7. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- Las funciones claves que generalmente lleva a cabo un protocolo comprenden el encapsulamiento, la fragmentación y el reensamblado, el control de la conexión, la entrega ordenada, el control de flujo, el control de errores, el direccionamiento y la multiplexación.
- Un conjunto de redes consta de múltiples redes separadas que están interconectadas por dispositivos de encaminamiento. Los datos se intercambian en paquetes entre un sistema origen y un destino a través de un camino que involucra múltiples redes y dispositivos de encaminamiento. Normalmente se utiliza un modo de operación no orientado a conexión o datagrama. Un dispositivo de encaminamiento acepta datagramas y los retransmite hacia su destino y es responsable de determinar la ruta, del mismo modo en el que actúa un nodo de conmutación de paquetes.
- El protocolo más comúnmente utilizado para la interconexión de redes es el Protocolo Internet (IP, *Internet Protocol*). IP incorpora una cabecera a los datos de la capa inmediatamente superior (por ejemplo, TCP) para formar un datagrama IP. La cabecera incluye las direcciones origen y destino, información utilizada para la fragmentación y el reensamblado, un campo de tiempo-de-vida, un campo de tipo de servicio y una suma de comprobación.
- Se ha definido un protocolo IP de nueva generación, conocido como IPv6. IPv6 proporciona campos de dirección más grandes y una mayor funcionalidad que el actual IP.

El propósito de este capítulo es examinar el Protocolo Internet, que constituye los fundamentos sobre los que se basan todos los protocolos de conjuntos de redes y la interconexión entre ellas. En primer lugar, será útil revisar las funciones básicas de los protocolos de red. Este repaso sirve para resumir parte del material introducido previamente y constituye un punto de comienzo en el estudio de los protocolos de interconexión de redes en la Parte V. A continuación, se expondrá una discusión sobre la interconexión de redes. El resto del capítulo está dedicado a los dos protocolos estándar de interconexión de redes: IPv4 e IPv6.

Se recomienda al lector repasar la Figura 2.15 para situar la posición de los protocolos que se discuten en este capítulo dentro del conjunto de protocolos TCP/IP.

18.1. FUNCIONES BÁSICAS DE LOS PROTOCOLOS

Antes de comenzar la discusión sobre los protocolos de interconexión de redes, consideremos un conjunto bastante pequeño de funciones que forman la base de todos los protocolos. No todos los protocolos poseen todas las funciones; esto implicaría una duplicación significativa del esfuerzo. Existen, no obstante, muchas instancias del mismo tipo de función presentes en los protocolos a distintos niveles.

Es posible agrupar las funciones de un protocolo dentro de las siguientes categorías:

- Encapsulamiento.
- Fragmentación y reensamblado.
- Control de conexión.
- Entrega ordenada.
- Control de flujo.

- Control de errores.
- Direccionamiento.
- Multiplexación.
- Servicios de transmisión.

ENCAPSULAMIENTO

Prácticamente en todos los protocolos, los datos son transferidos en bloques, llamados unidades de datos del protocolo (PDU, *Protocol Data Unit*). Cada PDU contiene no solo datos, sino también información de control. Ciertamente, algunas PDU constan únicamente de información de control sin datos algunos. La información de control se puede clasificar en tres categorías generales:

- **Dirección:** la dirección del emisor y/o destinatario debe ser indicada.
- **Código de detección de errores:** se suele incluir algún tipo de secuencia de comprobación de la trama para detectar la ocurrencia de errores.
- **Control del protocolo:** se incluye información adicional para implementar las funciones de los protocolos enumeradas en lo que resta de esta sección.

La adición de información de control a los datos es lo que se conoce como **encapsulamiento**. Los datos son aceptados o generados por una entidad y encapsulados dentro de una PDU que contiene los datos más información de control. Numerosos ejemplos de PDU han aparecido en los capítulos precedentes (por ejemplo, TFTP (*véase* Figura 2.17), HDLC (*véase* Figura 7.7), retransmisión de tramas (*véase* Figura 10.19), ATM (*véase* Figura 11.4), AAL5 (*véase* Figura 11.15), LLC (*véase* Figura 15.7), IEEE 802.3 (*véase* Figura 16.3), IEEE 802.11 (*véase* Figura 17.8)).

FRAGMENTACIÓN Y REENSAMBLADO[1]

Un protocolo se encarga del intercambio de flujos de datos entre dos entidades. Normalmente, la transferencia puede caracterizarse como una secuencia de PDU de algún tamaño acotado. En el nivel de aplicación, nos referimos a una unidad lógica de transferencia de datos como un mensaje. Independientemente de si la aplicación envía datos en mensajes o lo hace como un flujo continuo, los protocolos de niveles inferiores necesitarán separar los datos en bloques de un tamaño más reducido. Este proceso se denomina fragmentación.

En función del contexto, existe una serie de motivos para llevar a cabo la fragmentación. Algunas de las razones típicas para fragmentar se enumeran a continuación:

- La red de comunicaciones puede aceptar únicamente bloques de datos de un cierto tamaño como máximo. Por ejemplo, una red ATM está limitada a bloques de 53 octetos; Ethernet impone un tamaño máximo de 1526 octetos.
- El control de errores puede ser más eficiente con un tamaño de PDU más pequeño. Con PDU pequeñas se necesitan retransmitir menos bits cuando una PDU sufre un error.

[1] El término *segmentación* se utiliza en los documentos OSI, pero en la especificación de los protocolos relativos a TCP/IP se usa el término *fragmentación*. El significado de ambos es el mismo.

- Es posible proporcionar un acceso más equitativo y con menor retardo a los equipos de transmisión compartidos. Por ejemplo, sin un tamaño máximo de bloque, una estación podría monopolizar un medio multipunto.
- Un tamaño de PDU más pequeño supone que las entidades receptoras pueden reservar memorias temporales más pequeñas.
- Una entidad puede requerir que la transferencia de datos alcance algún tipo de terminación de vez en cuando, para efectuar controles y operaciones de reinicio/recuperación.

Existen varias desventajas en el uso de la fragmentación que hacen considerar tamaños de PDU tan grandes como sea posible:

- Como se acaba de explicar, cada PDU contiene una cierta cantidad de información de control. Por tanto, cuanto menor sea el bloque, mayor será el porcentaje de sobrecarga introducida.
- La llegada de una PDU puede generar una interrupción que debe ser atendida. A medida que el bloque sea más pequeño se generarán más interrupciones.
- Se requiere más tiempo para procesar muchas y pequeñas PDU.

Todos estos factores deben ser tomados en consideración por el diseñador de protocolos a la hora de determinar los tamaños de PDU máximos y mínimos.

El proceso inverso a la fragmentación es el reensamblado. Los datos segmentados pueden eventualmente ser reensamblados en mensajes apropiados en el nivel de aplicación. Si las PDU llegan fuera de orden, la tarea se complica.

El proceso de la fragmentación se ilustra en la Figura 2.4.

CONTROL DE CONEXIÓN

Una entidad puede transmitir datos a otra entidad de tal forma que cada PDU sea tratada independientemente de sus predecesoras. Esto se conoce como transferencia de datos no orientada a conexión; un ejemplo es el uso del datagrama, descrito en el Capítulo 10. Pese a que este modo es útil, una técnica igualmente importante es la transferencia de datos orientada a conexión, de la cual el circuito virtual, también descrito en el Capítulo 10, es un ejemplo.

La transferencia orientada a conexión se prefiere (incluso se requiere) si las estaciones anticipan un intercambio de datos voluminoso y/o ciertos detalles del protocolo deben funcionar dinámicamente. Una asociación lógica, o conexión, se establece entre las entidades. Se suceden tres etapas (*véase* Figura 18.1):

- Establecimiento de la conexión.
- Transferencia de datos.
- Terminación de la conexión.

En protocolos más sofisticados pueden existir también fases de interrupción y recuperación de la conexión para hacer frente a los errores y otros tipos de interrupciones.

Durante la etapa de establecimiento de la conexión, dos entidades aceptan intercambiar datos. Generalmente, una estación emitirá una solicitud de conexión (de forma no orientada a conexión) hacia la otra. Es posible que una autoridad central esté involucrada. En los protocolos más simples,

la entidad receptora acepta o rechaza la solicitud y, en el primero de los casos, la conexión se considera establecida. En propuestas más complejas, esta fase incluye una negociación en lo tocante a la sintaxis, semántica y temporización del protocolo. Por supuesto, ambas entidades deben utilizar el mismo protocolo. Pero el protocolo puede permitir ciertas funcionalidades opcionales y éstas deben ser consensuadas mediante una negociación. Por ejemplo, el protocolo puede especificar un tamaño de PDU de hasta 8.000 octetos; una estación puede desear restringir este tamaño a 1.000 octetos.

Tras el establecimiento de la conexión se entra en la etapa de transferencia de datos. Durante esta fase se intercambian datos e información de control (por ejemplo, control de flujo y control de errores). La Figura 18.1 muestra una situación en la cual todos los datos fluyen en un sentido, con acuses de recibos devueltos en el otro. Más generalmente, tanto los datos como los acuses de recibo fluyen en ambos sentidos. Finalmente, una de las partes desea terminar la conexión y lo hace enviando una solicitud de terminación. Alternativamente, una autoridad central podría terminar la conexión forzosamente.

Una característica clave de muchos protocolos de transferencia de datos orientados a conexión es la utilización de secuenciación (por ejemplo, HDLC e IEEE 802.11). Cada una de las partes numera secuencialmente las PDU que envía a la otra. Dado que cada parte recuerda que se encuentra en una conexión lógica, puede mantener una lista de los números salientes que genera y los números entrantes producidos por la otra parte. Ciertamente, uno puede definir en esencia una transferencia de datos orientada a conexión como aquella en la que ambas partes numeran las PDU y mantienen un registro de los números salientes y entrantes. La secuenciación es la base para tres funciones básicas: entrega ordenada, control de flujo y control de errores.

La secuenciación no se encuentra presente en todos los protocolos orientados a conexión. Algunos ejemplos son la retransmisión de tramas y ATM. Sin embargo, todos los protocolos orientados a conexión incluyen en el formato de la PDU alguna forma de identificar la conexión, bien mediante un identificador único o bien mediante una combinación de las direcciones del origen y el destino.

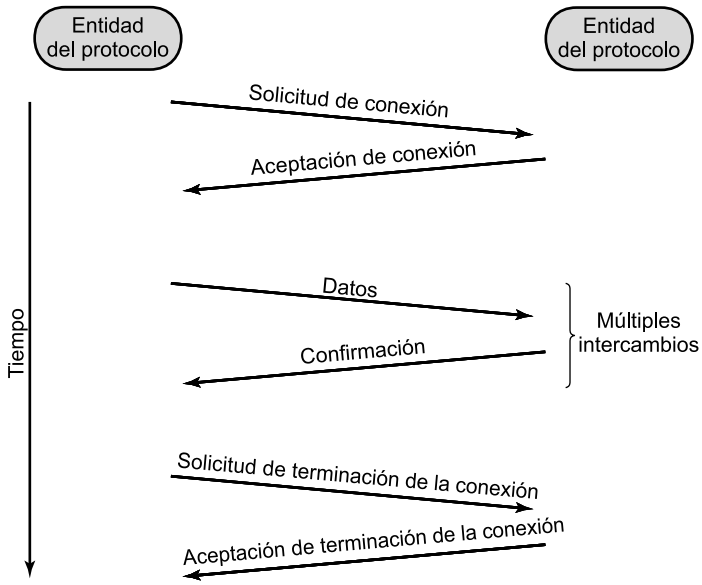


Figura 18.1. Etapas de una transferencia de datos orientada a conexión.

ENTREGA ORDENADA

Si dos entidades comunicantes se encuentran en diferentes anfitriones[2] (*hosts*) conectados por una red, existe el riesgo de que las PDU no lleguen a su destino en el orden en que fueron enviadas debido a la posibilidad de que atraviesen caminos diferentes a través de la red. En los protocolos orientados a conexión se requiere generalmente que el orden de las PDU se mantenga. Por ejemplo, si un archivo es transferido entre dos sistemas, sería deseable que se asegurara que los registros del archivo recibido están en el mismo orden que los del archivo transmitido, y no mezclados. Si cada PDU recibe un número único y los números se asignan secuencialmente, lógicamente es una tarea simple para la entidad receptora el reordenar las PDU recibidas basándose en los números de secuencia. Un problema con este esquema es que, con un campo de número de secuencia finito, los números se repiten (módulo algún número máximo). Evidentemente, el número máximo de secuencia debe ser mayor que el máximo número de PDU que podrían estar pendientes en cualquier instante de tiempo. De hecho, se puede necesitar que el número máximo sea el doble que el máximo número de PDU que puedan estar pendientes (por ejemplo, ARQ de repetición selectiva; *véase* Capítulo 7).

CONTROL DE FLUJO

El control de flujo es una función realizada por una entidad receptora para limitar la cantidad o la tasa de datos que es enviada por una entidad transmisora.

La forma más simple de control de flujo es un procedimiento de parada y espera, en el cual la recepción de cada PDU debe ser confirmada antes de que la siguiente sea enviada. Protocolos más eficientes incluyen algún tipo de crédito proporcionado al emisor, que es la cantidad de datos que pueden ser enviados sin acuse de recibo. La técnica de ventana deslizante de HDLC es un ejemplo de este mecanismo (*véase* Capítulo 7).

El control de flujo es un buen ejemplo de una función que debe ser implementada en varios protocolos. Considérese una vez más la Figura 2.3. La red necesitará efectuar un control de flujo sobre X a través del protocolo de acceso a la red para forzar el control sobre el tráfico de red. Al mismo tiempo, el módulo de acceso a la red Y posee únicamente un espacio limitado de memoria temporal y necesita efectuar un control de flujo sobre el módulo de acceso a la red X empleando el protocolo de transporte. Finalmente, aunque el módulo de acceso a la red Y pueda controlar su flujo de datos, la aplicación de Y puede ser vulnerable a un desbordamiento. Por ejemplo, la aplicación podría suspenderse mientras espera espacio en disco. Así, el control de flujo debe aplicarse también a los protocolos orientados a aplicación.

CONTROL DE ERRORES

Las técnicas de control de errores son necesarias para la prevención frente a pérdidas y daños en los datos y la información de control. El control de errores se implementa generalmente como dos funciones separadas: detección de errores y retransmisión. Para conseguir la detección de errores, el emisor inserta un código de detección de errores en la PDU transmitida, que es una función de los otros bits en la PDU. El receptor comprueba el valor del código en la PDU recibida. Si se detecta un error, el receptor descarta la PDU. En caso de no recibir el acuse de recibo de la PDU

[2] El término *anfitrión* alude a cualquier sistema final conectado a una red, como un PC, una estación de trabajo o un servidor.

en un tiempo razonable, el emisor la retransmite. Algunos protocolos emplean también un código de corrección de errores, que habilita al receptor no sólo para detectar errores sino para corregirlos en algunos casos.

Al igual que con el control de flujo, el control de errores es una función que debe ser realizada en varias capas de protocolos. Considérese de nuevo la Figura 2.3. El protocolo de acceso a la red debería incluir el control de errores para asegurar que los datos se intercambian correctamente entre la estación y la red. Sin embargo, un paquete de datos puede perderse dentro de la red y el protocolo de transporte debería ser capaz de recuperarse ante la pérdida.

DIRECCIONAMIENTO

El concepto de direccionamiento en una arquitectura de comunicaciones es una noción compleja y abarca una serie de cuestiones, incluyendo:

- Nivel de direccionamiento.
- Alcance del direccionamiento.
- Identificadores de conexión.
- Modo de direccionamiento.

Durante la discusión, ilustraremos los conceptos utilizando la Figura 18.2, que repite la Figura 2.13 y muestra una configuración utilizando la arquitectura TCP/IP. Los conceptos son esencialmente los mismos que para la arquitectura OSI o cualquier otra arquitectura de comunicaciones.

El **nivel de direccionamiento** se refiere al nivel en la arquitectura de comunicaciones en el cual una entidad es designada. Generalmente se asocia una dirección única con cada sistema final

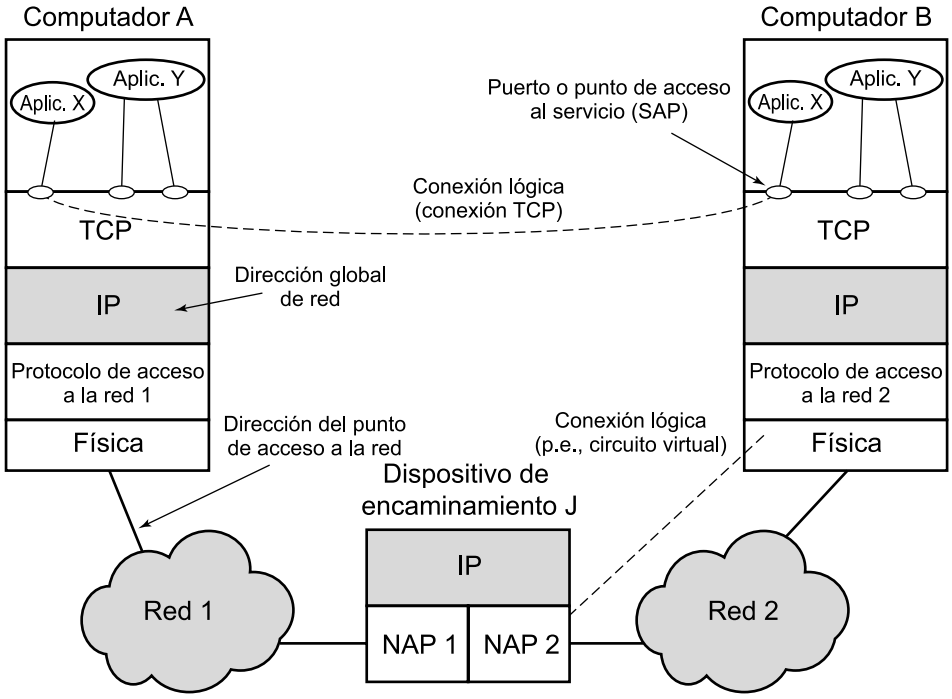


Figura 18.2. Conceptos TCP/IP.

(por ejemplo, una estación de trabajo o un servidor) y cada sistema intermedio (por ejemplo, un dispositivo de encaminamiento) en la configuración. Tal dirección es, en general, una dirección en el nivel de red. En el caso de la arquitectura TCP/IP, ésta es referida como dirección IP o, simplemente, dirección internet. En el caso de la arquitectura OSI, nos referimos a ella como punto de acceso al servicio de red (NSAP, *Network Service Access Point*). La dirección en el nivel de red se utiliza para encaminar una PDU a través de una o varias redes hasta el sistema indicado por la dirección en el nivel de red contenida en la PDU.

Una vez que los datos alcanzan el sistema destino, éstos deben ser dirigidos a algún proceso o aplicación en el sistema. Generalmente, un sistema soporta múltiples aplicaciones y una aplicación soporta varios usuarios. Cada aplicación, y quizá cada usuario concurrente de una aplicación, recibe un identificador único denominado puerto en la arquitectura TCP/IP y punto de acceso al servicio (SAP, *Service Access Point*) en la arquitectura OSI. Por ejemplo, un sistema podría soportar tanto una aplicación de correo electrónico como una de transferencia de archivos. Cada aplicación debería tener como mínimo un número de puerto o SAP que fuese único dentro del sistema. Además, la aplicación de transferencia de archivos podría soportar múltiples transferencias simultáneas, en cuyo caso a cada transferencia se le asignaría dinámicamente un número de puerto o SAP único.

La Figura 18.2 ilustra dos niveles de direccionamiento dentro de un sistema. Éste es generalmente el caso en la arquitectura TCP/IP. No obstante, podría existir direccionamiento en cada una de las capas de una arquitectura. Por ejemplo, se podría asignar un SAP único en cada nivel de la arquitectura OSI.

Otra cuestión relacionada con la dirección de un sistema final o intermedio es el **alcance del direccionamiento**. La dirección internet o dirección NSAP referida previamente es una dirección global. Las características clave de una dirección global son las siguientes:

- **Ausencia de ambigüedad global:** una dirección global identifica únicamente un sistema. Se permiten los sinónimos. Esto es, un sistema puede tener más de una dirección global.
- **Aplicabilidad global:** es posible que desde cualquier dirección global se identifique cualquier otra dirección global, ubicada en cualquier sistema, mediante la utilización de la dirección global del otro sistema.

Dado que una dirección global es única y aplicable globalmente, permite a una colección de redes encaminar datos procedentes de cualquier sistema conectado a una red hacia otro sistema conectado a cualquier otra red.

La Figura 18.2 ilustra que podría requerirse otro nivel de direccionamiento. Cada red debe mantener una dirección única para cada interfaz de dispositivo en la red. Ejemplos de ello son las direcciones MAC en una red IEEE 802 y las direcciones de anfitriones en ATM. Esta dirección permite a la red encaminar unidades de datos (por ejemplo, tramas MAC y celdas ATM) a través de la red y entregarlas al sistema pertinente. Podemos referirnos a tales direcciones como *direcciones del punto de acceso a la red*.

Generalmente, la cuestión del alcance del direccionamiento es sólo relevante para direcciones en el nivel de red. Un puerto o SAP por encima del nivel de red es único dentro de un sistema dado pero no necesita ser globalmente único. Por ejemplo, en la Figura 18.2 puede haber un puerto 1 en el sistema A y un puerto 1 en el sistema B. La designación completa de estos dos puertos podría ser expresada como A.1 y B.1, que son nombres únicos.

El concepto de **identificadores de conexión** aparece en escena cuando consideramos transferencias orientadas a conexión (por ejemplo, circuitos virtuales) en lugar de transferencias no orien-

tadas a conexión (por ejemplo, datagramas). En transferencias no orientadas a conexión se utiliza un identificador global para cada transmisión de datos. En el caso de las transferencias orientadas a conexión, es deseable en algunas ocasiones usar solamente un identificador de conexión durante la fase de transferencia de datos. El escenario es éste: la entidad 1 en el sistema A solicita una conexión a la entidad 2 en el sistema B, usando quizá la dirección global B.2. Cuando B.2 acepta la conexión se proporciona un identificador de conexión (normalmente un número) que es usado por ambas entidades para futuras transmisiones. El uso de un identificador de conexión presenta varias ventajas:

- **Reducción de la sobrecarga:** los identificadores de conexión son generalmente más cortos que los identificadores globales. Por ejemplo, en el protocolo de retransmisión de tramas (analizado en el Capítulo 10), los paquetes de solicitud de conexión contienen campos para la dirección de origen y la dirección de destino. Tras el establecimiento de la conexión lógica, denominada conexión de enlace de datos, las tramas de datos contienen un identificador de conexión del enlace de datos (DLCI, *Data Link Connection Identifier*) de 10, 16 o 23 bits.
- **Encaminamiento:** en la configuración de una conexión se puede definir una ruta fija. El identificador de la conexión sirve para identificar la ruta en los sistemas intermedios, como nodos de conmutación de paquetes, para manejar las futuras PDU.
- **Multiplexación:** trataremos esta función en términos más generales después. Aquí haremos la observación de que una entidad puede desear disfrutar de más de una conexión simultáneamente. Así, las PDU entrantes deben ser identificadas por su identificador de conexión.
- **Uso de información de estado:** una vez que una conexión está establecida, los sistemas finales pueden mantener información de estado concerniente a la misma. Esto permite funciones como el control de flujo y el control de errores utilizando números de secuencia. Vemos ejemplos de esto con HDLC (*véase* Capítulo 7) e IEEE 802.11 (*véase* Capítulo 17).

La Figura 18.2 muestra varios ejemplos de conexiones. La conexión lógica entre el dispositivo de encaminamiento J y el computador B se produce en el nivel de red. Por ejemplo, si la red 2 es una red de retransmisión de tramas, entonces esta conexión lógica sería una conexión de enlace de datos. En niveles superiores, muchos protocolos en el nivel de transporte, como TCP, soportan las conexiones lógicas entre usuarios del servicio de transporte. Así, TCP puede mantener una conexión entre dos puertos situados en sistemas diferentes.

Otro concepto de direccionamiento es el de **modo de direccionamiento**. En su forma más común, una dirección se refiere a un sistema individual o a un puerto; en este caso nos referiremos a ella como una dirección individual o **unidifusión** (*unicast*). Es también posible que una dirección se refiera a más de una entidad o puerto. Tal dirección identifica simultáneamente a múltiples receptores para los datos. Por ejemplo, un usuario podría desear enviar unos apuntes a una serie de personas. El centro de control de red podría querer notificar a todos los usuarios que la red va a venirse abajo. Una dirección para múltiples receptores puede ser de **difusión** (*broadcast*), destinada a todas las entidades dentro de un dominio, o de **multidistribución** (*multicast*), para un subconjunto específico de entidades. La Tabla 18.1 ilustra los casos posibles.

MULTIPLEXACIÓN

Relacionado con el concepto de direccionamiento se encuentra el de multiplexación. Una forma de multiplexación es soportada mediante múltiples conexiones en un solo sistema. Por ejemplo, con retransmisión de tramas pueden existir varias conexiones de enlace de datos que terminen en el

Tabla 18.1. Modos de direccionamiento.

Destino	Dirección de red	Dirección de sistema	Dirección de puerto/SAP
Unidifusión (*unicast*)	Individual	Individual	Individual
Multidifusión (*multicast*)	Individual Individual Todos	Individual Todos Todos	Grupo Grupo Grupo
Difusión (*broadcast*)	Individual Individual Todos	Individual Todos Todos	Todos Todos Todos

mismo sistema; podemos decir que estas conexiones de enlace de datos son multiplexadas sobre la interfaz física individual que existe entre el sistema final y la red. La multiplexación puede realizarse también mediante números de puerto, lo cual permite también múltiples conexiones simultáneas. Por ejemplo, puede haber varias conexiones TCP que finalicen en un sistema dado, cada una establecida entre un par de puertos diferentes.

La multiplexación es usada igualmente en otro contexto, referente a la asignación de conexiones de un nivel a otro. Considérese de nuevo la Figura 18.2. La red 1 podría proporcionar un servicio orientado a conexión. Para cada conexión proceso a proceso establecida en el siguiente nivel, una conexión de enlace de datos podría ser creada en el nivel de acceso a la red. Ésta es una relación uno a uno, pero no tiene por qué ser así necesariamente. La multiplexación puede usarse en una de dos direcciones. La multiplexación ascendente, o hacia dentro, ocurre cuando múltiples conexiones de un nivel superior son multiplexadas sobre, o comparten, una única conexión de más bajo nivel. Esto puede ser necesario para hacer un uso más eficiente de los servicios de niveles inferiores o para proporcionar varias conexiones en niveles superiores dentro de un entorno en el que sólo existe una conexión en niveles inferiores. La multiplexación descendente, o división, significa que una conexión individual de un nivel superior se sustenta sobre múltiples conexiones de niveles inferiores, siendo repartido el tráfico de la conexión superior entre las distintas conexiones inferiores. Esta técnica puede ser utilizada para proporcionar fiabilidad, rendimiento o eficiencia.

SERVICIOS DE TRANSMISIÓN

Un protocolo puede proporcionar una variedad de servicios adicionales a las entidades que lo usan. Mencionamos aquí tres ejemplos comunes:

- **Prioridad:** ciertos mensajes, como los de control, pueden necesitar llegar a la entidad destino con un retardo mínimo. Un ejemplo sería una solicitud de terminación de la conexión. Así, la prioridad podría ser asignada en función del mensaje. Adicionalmente, se podría asignar en función de la conexión.
- **Calidad de servicio:** ciertas clases de datos pueden requerir un umbral de rendimiento mínimo o un umbral de retardo máximo.
- **Seguridad:** los mecanismos de seguridad, restringiendo el acceso, pueden ser invocados.

Todos estos servicios dependen del sistema subyacente de transmisión y de cualquier entidad de niveles inferiores que intervenga. Si es posible que estos servicios sean proporcionados desde abajo, las dos entidades podrán hacer uso de ellos mediante el protocolo.

18.2. PRINCIPIOS DE LA INTERCONEXIÓN ENTRE REDES

Las redes de conmutación de paquetes y las de difusión de paquetes crecieron ante la necesidad de permitir a los usuarios de computadores tener acceso a los recursos existentes más allá de los que se disponen en un único sistema. De una forma similar, los recursos de una única red son a menudo insuficientes para satisfacer las necesidades de los usuarios. Ya que las redes que podrían ser de interés exhiben muchas diferencias, no es práctico tratar de agruparlas todas en una única red. Más bien, lo que se necesita es la habilidad de interconectar varias redes para que se puedan comunicar dos estaciones cualesquiera de cualquier red.

La Tabla 18.2 muestra algunos de los términos más comúnmente utilizados y relacionados con la interconexión entre redes (*internetworking*). Un conjunto de redes interconectadas, desde el punto de vista del usuario, puede aparecer simplemente como una red más grande. Sin embargo, si cada una de las redes constituyentes retiene su identidad y se necesitan mecanismos especiales para la comunicación a través de múltiples redes, entonces a la configuración entera se le conoce como **conjunto de redes** (o **una internet**).

Tabla 18.2. Terminología de interconexión entre redes.

Red de comunicación
Un sistema que proporciona un servicio de transferencia de datos entre estaciones conectadas a la red.

Internet
Una colección de redes de comunicación interconectadas por puentes o dispositivos de encaminamiento.

Intranet
Una *internet* corporativa que proporciona las aplicaciones claves de Internet, especialmente el *world wide web*. Una intranet opera dentro de una organización con fines internos y puede existir aisladamente, como una internet autocontenida o puede tener enlaces a Internet.

Subred
Hace referencia a una red constituyente de una internet. Esto evita la ambigüedad dado que, desde el punto de vista del usuario, una internet completa es una sola red.

Sistema Final (ES)
Un dispositivo conectado a una de las redes de una internet que se utiliza para apoyar a las aplicaciones o servicios del usuario final.

Sistema Intermedio (IS)
Un dispositivo utilizado para conectar dos redes y permitir la comunicación entre sistemas finales conectados a diferentes redes.

Puente (*bridge*)
Un IS utilizado para conectar dos redes LAN que utilizan el mismo protocolo LAN. El puente actúa como un filtro de direcciones, recogiendo paquetes de una LAN que van dirigidos a un destino en otra LAN y pasándolos hacia adelante. El puente no modifica el contenido del paquete ni incorpora nada al mismo. Opera en la capa 2 del modelo OSI.

Dispositivo de encaminamiento (*router*)
Un IS utilizado para conectar dos redes que pueden o no ser similares. El dispositivo de encaminamiento utiliza un protocolo de internet presente en cada dispositivo de encaminamiento y en cada computador de la red. Opera en la capa 3 del modelo OSI.

Cada red constituyente de una internet permite la comunicación entre los dispositivos conectados a esa red; estos dispositivos se conocen como **sistemas finales** (ES, *End Systems*). Además, las redes se conectan por dispositivos denominados en los documentos ISO como **sistemas intermedios** (IS, *Intermediate Systems*). Los IS proporcionan caminos de comunicación y realizan las

funciones de retransmisión y encaminamiento necesarias para que los datos se puedan intercambiar entre los dispositivos conectados en las diferentes redes de la internet.

Existen dos tipos de IS, los puentes y los dispositivos de encaminamiento, que son de particular interés. Las diferencias entre ellos se derivan de los protocolos utilizados para la lógica de la interconexión entre las redes. En esencia, un **puente** opera en la capa 2 de la arquitectura de 7 capas del modelo para la interconexión de sistemas abiertos (OSI) y actúa como un retransmisor de tramas entre redes parecidas; los puentes ya se examinaron en detalle en el Capítulo 15. Un **dispositivo de encaminamiento** opera en la capa 3 de la arquitectura OSI y encamina los paquetes entre redes potencialmente diferentes. Tanto los puentes como los dispositivos de encaminamiento suponen que se usa el mismo protocolo en la capa superior.

Comenzaremos nuestro estudio de la interconexión de redes con una discusión de los principios subyacentes en varios enfoques de interconexión entre redes. Después examinaremos la técnica más importante para la interconexión entre redes: el dispositivo de encaminamiento no orientado a conexión. Tras ello se describe el protocolo para la interconexión más extendido, llamado sencillamente Protocolo Internet (del inglés *Internet Protocol*, IP). A continuación, se examina el protocolo de interconexión normalizado más reciente, conocido como IPv6.

REQUISITOS

Los requisitos globales para un sistema de interconexión entre redes son los que siguen a continuación:

1. Proporcionar un enlace entre redes. Como mínimo, se necesita una conexión física y de control del enlace.
2. Proporcionar el encaminamiento y entrega de los datos entre procesos en diferentes redes.
3. Proporcionar un servicio de contabilidad que realice un seguimiento de la utilización de las diferentes redes y dispositivos de encaminamiento y mantenga información de estado.
4. Proporcionar los servicios mencionados de forma que no se requiera la modificación de la arquitectura de red de cualquiera de las redes interconectadas. Esto significa que el sistema de interconexión entre redes se debe acomodar a las diversas diferencias existentes entre las distintas redes. Algunas de estas diferencias son:
   - **Diferentes esquemas de direccionamiento:** las redes pueden usar diferentes nombres y direcciones de los puntos finales y diferentes esquemas de mantenimiento del directorio. Por tanto, se debe proporcionar un esquema de direccionamiento de red global así como un servicio de directorio.
   - **Diferente tamaño máximo de paquete:** puede que se necesite romper un paquete en unidades más pequeñas al pasar a otra red. Este proceso se denomina fragmentación.
   - **Diferentes mecanismos de acceso a la red:** el mecanismo de acceso de la estación a la red podría ser diferente para estaciones de redes diferentes.
   - **Diferentes valores de expiración de los temporizadores:** normalmente, un servicio de transporte orientado a conexión esperará la confirmación de una recepción correcta de datos hasta que un temporizador expira, en cuyo caso retransmitirá su bloque de datos. En general, se requieren valores grandes del temporizador para realizar una entrega satisfactoria a través de redes múltiples. Los procedimientos que establecen los valores en la interconexión de redes deben permitir una transmisión satisfactoria que evite retransmisiones innecesarias.

- **Recuperación de errores:** los procedimientos deben proporcionar un servicio que va desde no suministrar recuperación de errores hasta un servicio extremo a extremo (dentro de la red) seguro. El servicio de interconexión de redes no debería depender o no tendría que ser interferido por la naturaleza de la capacidad de recuperación de errores de las redes individuales.
- **Informes de estado:** las diferentes redes dan informes de estado y de rendimiento de una forma diferente. Debe ser posible que el sistema de interconexión proporcione información de la actividad de interconexión a los procesos interesados y autorizados.
- **Técnicas de encaminamiento:** el encaminamiento dentro de la red puede depender de la detección de fallos y de las técnicas de control de congestión particulares de cada red. El sistema de interconexión entre redes debe ser capaz de coordinar estas técnicas para encaminar los datos adaptativamente entre las estaciones de las diferentes redes.
- **Control de acceso del usuario:** cada red tendrá su propia técnica de control de acceso de los usuarios (autorización para usar la red). Estas técnicas se deben solicitar por el sistema de interconexión según se necesite. Además, se podría requerir una técnica diferente de control de acceso a la interconexión entre redes.
- **Conexión, sin conexión:** las redes individuales pueden proporcionar un servicio orientado a conexión (por ejemplo, circuitos virtuales) o no orientados a conexión (datagramas). Es deseable que el servicio entre redes no dependa de la naturaleza del servicio de conexión de las redes individuales.

Algunos de estos requisitos los satisface el protocolo de Internet (IP). Otros requieren un control adicional y software de aplicación, como se verá en este capítulo y en el siguiente.

ENFOQUES SOBRE LA ARQUITECTURA

Una característica clave en una arquitectura de interconexión de redes es si el modo de operación es orientado a conexión o no orientado a conexión.

Funcionamiento orientado a conexión

En el modo de operación orientado a conexión se supone que cada red proporciona un servicio en forma de conexión. Esto es, se establece una conexión lógica a nivel de red (por ejemplo, circuito virtual) entre cualquier par de sistemas finales (ES) conectados a la misma red. Primero se establece la conexión, y a continuación se produce el intercambio de datos. Con esta idea en mente, podemos resumir la opción de operación orientada a conexión como sigue:

1. Los IS se utilizan para conectar dos o más subredes; cada IS aparece como un ES en cada una de las redes a las que está conectado.
2. Cuando el ES A quiere intercambiar datos con el ES B, se establece una conexión lógica entre ellos. Esta conexión lógica consiste en la concatenación de una secuencia lógica de conexiones a través de subredes. Esta secuencia es tal que forma un camino desde el ES A al ES B.
3. Las conexiones lógicas individuales dentro de una red están realizadas por varios IS. Cualquier tráfico que llega a un IS en una conexión lógica se retransmite en una segunda conexión lógica y viceversa.

No siempre se da el caso de que las redes constituyentes de un conjunto de redes proporcionen un servicio orientado a conexión. Por ejemplo, una red de área local IEEE 802 proporciona un servi-

cio definido por el control lógico del enlace (LLC). Dos de las opciones de LLC proporcionan servicios no orientados a conexión. Por tanto, en realidad estas redes tienen un estilo de transmisión estilo datagrama. Así, en este caso, el servicio de la red se debe mejorar. Un ejemplo de cómo se podría realizar esto es que los IS implementen X.25 encima de LLC a través de la LAN.

Un IS orientado a conexión realiza las siguientes funciones claves:

- **Retransmisión:** las unidades de datos que llegan de una red vía el protocolo de la capa de red se retransmiten a otra red. El tráfico se conduce a través de conexiones lógicas que están enlazadas por los IS.
- **Encaminamiento:** cuando se va a establecer una conexión lógica extremo a extremo, consistente en una secuencia de conexiones lógicas, cada IS en la secuencia debe tomar una decisión de encaminamiento que determina el siguiente salto en la secuencia.

Así, en la capa 3 se realiza una operación de retransmisión. Se supone que todos los sistemas finales comparten protocolos comunes en la capa 4 (transporte) y superiores para obtener una comunicación extremo a extremo satisfactoria.

Un ejemplo del enfoque orientado a conexión es el estándar X.75, utilizado para interconectar redes de conmutación de paquetes X.25. En la práctica, el enfoque orientado a conexión no se utiliza normalmente. El enfoque dominante es el no orientado a conexión, utilizando IP.

Funcionamiento no orientado a conexión

Mientras que el modo de funcionamiento orientado a conexión se corresponde con el mecanismo de circuito virtual de una red de conmutación de paquetes (*véase* Figura 10.13), el modo de operación no orientado a conexión se corresponde con el mecanismo de datagramas de una red de conmutación de paquetes (*véase* Figura 10.12). Cada unidad de datos del protocolo de red se trata independientemente y se encamina desde el ES origen al ES destino a través de una serie de dispositivos de encaminamiento y redes. Para cada unidad de datos transmitida por A, A realiza una decisión sobre qué dispositivo de encaminamiento debería recibir la unidad de datos. La unidad de datos salta a través del conjunto de redes de un dispositivo de encaminamiento al siguiente hasta que alcanza la subred destino. En cada dispositivo de encaminamiento se toma una decisión de encaminamiento (independientemente para cada unidad de datos) relativa al siguiente salto. Así, diferentes unidades de datos pueden viajar por diferentes rutas entre el ES origen y destino.

Todos los ES y todos los dispositivos de encaminamiento comparten un protocolo de la capa de red común conocido genéricamente como protocolo de interconexión de redes. Dentro del proyecto internet de DARPA se desarrolló un protocolo Internet (IP) inicial, publicado como RFC 791, que ha llegado a ser un estándar de Internet. Existe la necesidad de disponer de un protocolo para acceder a cada red particular debajo de un protocolo de interconexión de redes. Así, normalmente hay dos protocolos en la capa de red operando en cada ES y dispositivo de encaminamiento: una subcapa superior que proporciona la función de interconexión y una capa inferior que proporciona el acceso a la red.

18.3. INTERCONEXIÓN ENTRE REDES SIN CONEXIÓN

En esta sección se examinan las funciones esenciales de un protocolo de interconexión. Por comodidad, nos vamos a referir concretamente al estándar de Internet IP, pero se debe entender que la narración de esta sección se aplica a cualquier protocolo de interconexión no orientado a conexión, como es el caso de IPv6.

FUNCIONAMIENTO DE UN ESQUEMA DE INTERCONEXIÓN NO ORIENTADO A CONEXIÓN

IP proporciona un servicio no orientado a conexión, o datagrama, entre sistemas finales. El enfoque sin conexión tiene una serie de ventajas. Éstas son:

- Un sistema de interconexión sin conexión es flexible. Puede trabajar con una gran variedad de redes, algunas de las cuales serán también sin conexión. En esencia, IP requiere muy poco de las redes sobre las que actúa.
- Un servicio de interconexión sin conexión se puede hacer bastante robusto. Se puede utilizar el mismo argumento expuesto para un servicio de red datagrama frente a un servicio con circuitos virtuales. Para una discusión en profundidad, se recomienda al lector la Sección 10.6.
- Un servicio de interconexión sin conexión es el mejor servicio para un protocolo de transporte no orientado a conexión, ya que no impone información suplementaria innecesaria.

La Figura 18.3 muestra un ejemplo típico en el que se usa IP, donde dos LAN se interconectan mediante una red WAN de retransmisión de tramas. La figura muestra el funcionamiento del protocolo IP para los datos intercambiados entre el computador A en una LAN (red 1) y el computador B en otra LAN (red 2) a través de la WAN. La figura muestra la arquitectura del protocolo y el formato de la unidad de datos en cada etapa. Los sistemas finales y los dispositivos de encaminamiento deben compartir un protocolo de interconexión común. Además, los sistemas finales deben compartir el mismo protocolo que hay encima de IP. Los dispositivos de encaminamiento intermedios sólo necesitan implementar hasta el protocolo IP.

El protocolo IP en A recibe bloques de datos desde las capas superiores del software en A para que los envíe a B. IP añade una cabecera (en el instante t_1) especificando, entre otras cosas, la dirección global Internet de B. Esa dirección consta de dos partes lógicas: un identificador de la red y un identificador del sistema final. La combinación de la cabecera IP y los datos de la capa superior se llama unidad de datos del protocolo de interconexión (PDU, *Protocol Data Unit*), o simplemente un datagrama (*véase* Figura 2.14). El datagrama es posteriormente encapsulado con el protocolo de la LAN (cabecera LLC en el instante t_2; cabecera y cola MAC en el instante t_3) y enviado al dispositivo de encaminamiento, que elimina la cabecera LAN para leer la cabecera IP (t_6). El dispositivo de encaminamiento, entonces, encapsula el datagrama con los campos del protocolo de retransmisión de tramas (t_8) y lo transmite a través de la WAN a otro dispositivo de encaminamiento. Este dispositivo de encaminamiento elimina los campos de retransmisión de tramas y recupera el datagrama, al cual se le incorporan los campos LAN apropiados de la LAN 2 y se envía a B.

Examinemos con más detalle este ejemplo. El sistema final A tiene que enviar un datagrama al sistema final B; el datagrama incluye la dirección internet de B. El módulo IP en A reconoce que el destino (B) está en otra subred. Por tanto, el primer paso es enviar los datos a un dispositivo de encaminamiento, en este caso al dispositivo de encaminamiento X. Para hacer esto, IP pasa el datagrama a la capa inferior (en este caso la capa LLC) con instrucciones para que se envíe al dispositivo de encaminamiento X. LLC pasa esta información a la capa MAC, que inserta la dirección de la capa MAC del dispositivo de encaminamiento en la cabecera MAC. Así, el bloque de datos transmitido en la LAN 1 incluye datos de una aplicación que está por encima de TCP, más la cabecera TCP, una cabecera IP, la cabecera LLC y la cabecera y cola MAC (tiempo t_3 en la Figura 18.3).

A continuación, el paquete viaja a través de la red 1 hasta el dispositivo de encaminamiento X. Éste elimina los campos MAC y LLC y analiza el campo IP para determinar el destino último

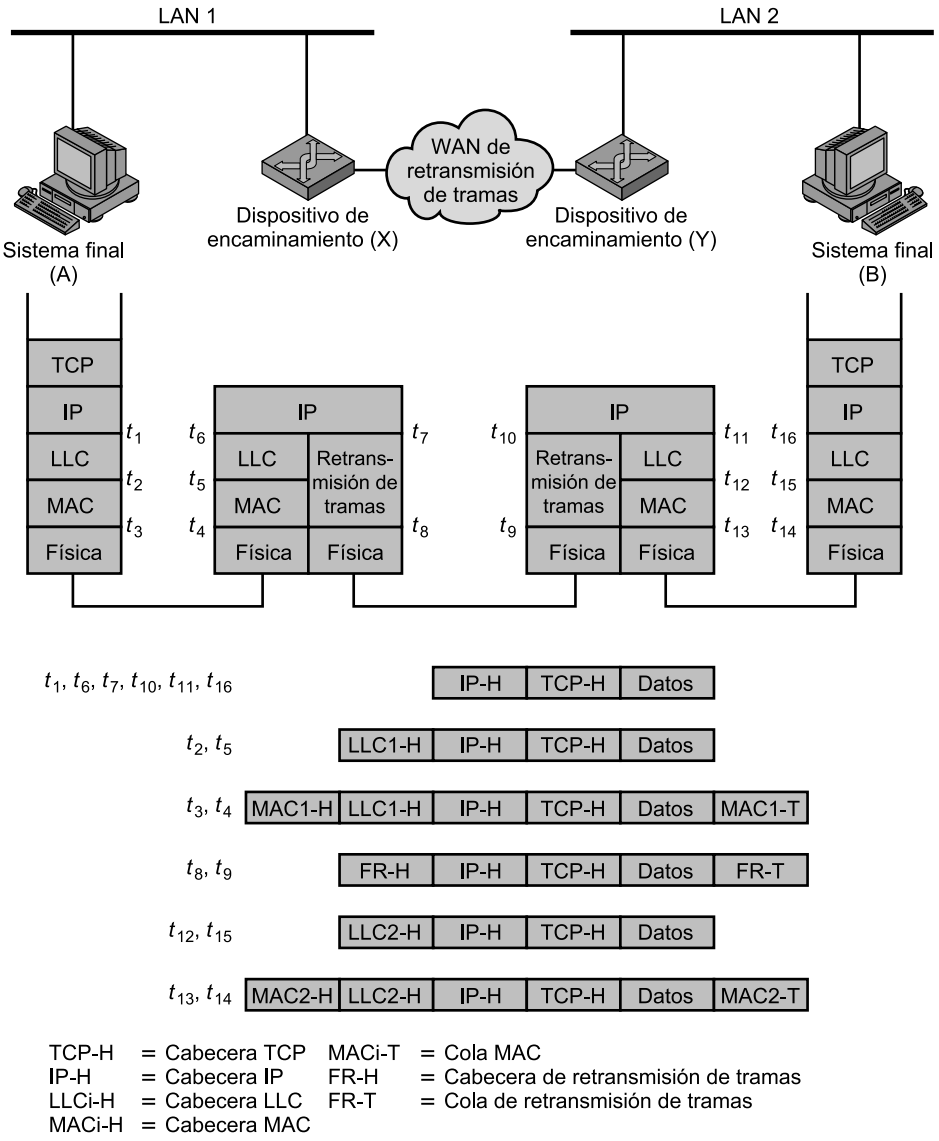


Figura 18.3. Funcionamiento del protocolo Internet.

de los datos, en este caso B. El encaminador debe tomar ahora una decisión de encaminamiento. Existen tres posibilidades:

1. La estación destino B está conectada directamente a una de las redes a las que el dispositivo de encaminamiento está conectado. En este caso, el dispositivo de encaminamiento envía el datagrama directamente al destino.

2. Se tienen que atravesar uno o más dispositivos de encaminamiento para alcanzar el destino. En este caso, se debe tomar una decisión de encaminamiento: ¿a qué dispositivo de encaminamiento se debe enviar el datagrama? En ambos casos 1 y 2, el módulo IP en el dispositivo de encaminamiento envía el datagrama a la capa inferior con la dirección de la

red de destino. Hay que indicar que aquí se está hablando de una dirección de una capa inferior referente a esta red.

3. El dispositivo de encaminamiento no conoce la dirección de destino. En este caso, el dispositivo de encaminamiento devuelve un mensaje de error a la fuente del datagrama.

En este ejemplo, los datos deben pasar a través del dispositivo de encaminamiento Y antes de alcanzar su destino. Por tanto, el dispositivo de encaminamiento X construye una nueva trama incorporando a la unidad de datos IP la cabecera y cola de retransmisión de tramas. La cabecera de retransmisión de tramas indica una conexión lógica con el dispositivo de encaminamiento Y; cuando esta trama llega al dispositivo de encaminamiento Y, se eliminan la cabecera y la cola. El dispositivo de encaminamiento determina que esta unidad de datos IP va dirigida a B, que está conectado directamente a la red a la cual está conectado el dispositivo de encaminamiento. Éste, por tanto, construye una trama con la dirección destino de la capa 2 de B y la envía en la LAN 2. Finalmente, los datos llegan a B, donde son eliminadas las cabeceras LAN e IP.

En cada dispositivo de encaminamiento, antes de que se reenvíen los datos, se podría necesitar fragmentar la unidad de datos para acomodarlos a la red de salida si en ésta hay un tamaño máximo de paquete inferior. La unidad de datos es partida en dos o más fragmentos, cada uno de los cuales constituirá una unidad de datos IP independiente. Cada nueva unidad de datos se integra en un paquete de la capa inferior y se coloca en cola para su transmisión. El dispositivo de encaminamiento podría también limitar la longitud de sus colas para cada red a la que está conectado para evitar que una red lenta perjudique a una rápida. Una vez que se alcanza el límite de la cola, las unidades de datos adicionales se descartan.

El proceso descrito antes continúa a través de tantos dispositivos de encaminamiento como necesite la unidad de datos para alcanzar su destino. Como con un dispositivo de encaminamiento, el sistema final destino recupera la unidad de datos IP a partir de los fragmentos obtenidos de la red. Si ha habido fragmentación, el módulo IP en el sistema final destino almacena temporalmente los datos que llegan hasta que el bloque original de datos pueda ser totalmente reensamblado. Después, este bloque de datos se pasa a la capa superior del sistema final.

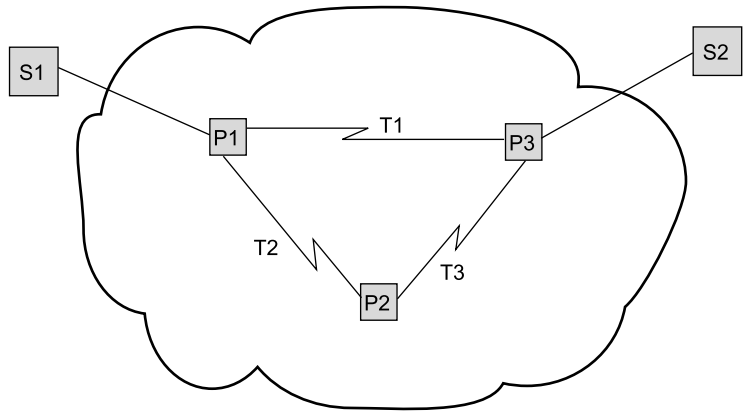
Este servicio ofrecido por un protocolo de interconexión es del tipo no fiable. Esto es, el protocolo de interconexión no garantiza que todos los datos se entreguen al destino ni que los datos que se entregan lleguen en el orden adecuado. Es responsabilidad de la capa superior (por ejemplo, TCP) tratar los errores que ocurran. Esta técnica proporciona un alto grado de flexibilidad.

Con esta forma de abordar el protocolo de interconexión, cada unidad de datos se pasa de dispositivo de encaminamiento a dispositivo de encaminamiento para ir de la fuente al destino. Puesto que la entrega no se garantiza, no hay ningún requisito particular de fiabilidad en cualquiera de las redes. Así, el protocolo funcionará con cualquier combinación de tipos de red. Ya que la secuencia de entrega no está garantizada, las unidades de datos sucesivas pueden seguir diferentes caminos a través del conjunto de redes. Esto le permite al protocolo reaccionar frente a la congestión y los fallos en las redes cambiando las rutas.

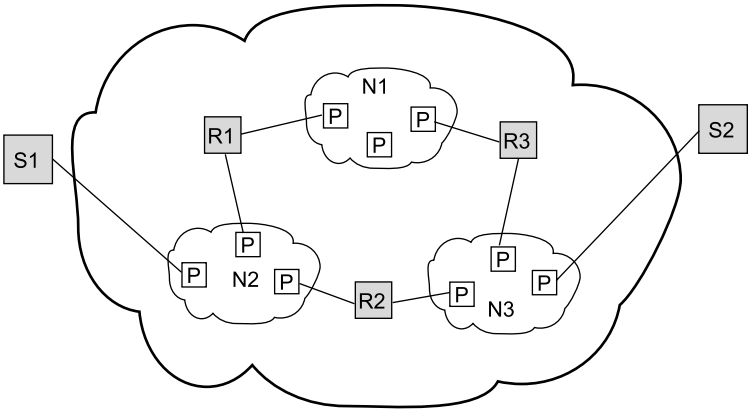
CUESTIONES DE DISEÑO

Con este breve esbozo del funcionamiento de una interconexión entre redes controlada por IP, podemos ahora volver atrás y examinar algunas cuestiones de diseño con un mayor detalle. Éstas son:

- Encaminamiento.
- Tiempo de vida de los datagramas.
- Segmentación y reensamblado.



(a) Arquitectura de red de conmutación de paquetes



(b) Arquitectura de interconexión

Figura 18.4. La interconexión como una red (basado en [HIND83]).

- Control de errores.
- Control de flujo.

Conforme desarrollemos esta discusión, el lector notará muchas similitudes con las cuestiones de diseño y las técnicas relevantes en una red de conmutación de paquetes. Para ver la razón de esto, considere la Figura 18.4 que compara una arquitectura de interconexión con una arquitectura de red de conmutación de paquetes. Los dispositivos de encaminamiento (R1, R2 y R3) en el conjunto de redes corresponden a los nodos de conmutación de paquetes (P1, P2 y P3) en la red, y las redes (N1, N2 y N3) en el conjunto de redes se corresponden con los enlaces de transmisión (T1, T2 y T3) en las redes. Los dispositivos de encaminamiento realizan esencialmente las mismas funciones que los nodos de conmutación de paquetes y usan las redes intermedias de una forma análoga a los enlaces de transmisión.

Encaminamiento

El encaminamiento se efectúa por medio del mantenimiento de una tabla de encaminamiento en cada dispositivo de encaminamiento y en cada sistema final. En esta tabla se da, para cada red

posible de destino, el siguiente dispositivo de encaminamiento al que se deberá enviar el datagrama internet.

La tabla de encaminamiento puede ser estática o dinámica. Una tabla estática puede contener rutas alternativas por si algún dispositivo de encaminamiento no está disponible. Una tabla dinámica es más flexible a la hora de enfrentarse a condiciones de error y congestión. En Internet, por ejemplo, cuando un dispositivo de encaminamiento se desconecta, todos sus vecinos emitirán un informe de estado, permitiendo a otros dispositivos de encaminamiento y estaciones que actualicen sus tablas de encaminamiento. Es posible utilizar un esquema similar para el control de congestión. Este último caso es particularmente importante a causa de las diferencias de capacidad entre las redes locales y las de área amplia. El Capítulo 19 discute los protocolos de encaminamiento.

Las tablas de encaminamiento también se pueden utilizar para ofrecer otros servicios de interconexión entre redes, como seguridad y prioridad. Por ejemplo, las redes individuales se podrían clasificar para gestionar datos de hasta un nivel de seguridad dado. El mecanismo de encaminamiento debe asegurar que a los datos de cierto nivel de seguridad no se les permita pasar a través de redes no acreditadas para gestionar tales datos.

Otra técnica de encaminamiento es el encaminamiento en el origen. La estación fuente especifica la ruta mediante la inclusión de una lista secuencial de dispositivos de encaminamiento en el datagrama. Esto, de nuevo, podría ser útil por motivos de seguridad o prioridad.

Finalmente, mencionaremos un servicio relacionado con el encaminamiento: el registro de la ruta. Para registrar la ruta, cada dispositivo de encaminamiento incorpora su dirección internet a una lista de direcciones que lleva el datagrama. Esta característica es útil con el objetivo de realizar operaciones de comprobación y depuración.

Tiempo de vida de los datagramas

Si se utiliza un encaminamiento dinámico o alternativo, existe la posibilidad de que un datagrama viaje indefinidamente a través del conjunto de redes. Esto no es aconsejable por dos razones. Primero, un datagrama circulando indefinidamente consume recursos. Segundo, como veremos en el Capítulo 20, un protocolo de transporte depende de la existencia de un límite en la vida de un datagrama. Para evitar estos problemas, cada datagrama se puede marcar con un tiempo de vida. Una vez que ha transcurrido este tiempo de vida, el datagrama se descarta.

Una forma sencilla de implementar esta función es usar un contador de saltos. Cada vez que un datagrama pasa a través de un dispositivo de encaminamiento, se decrementa el contador. Alternativamente, el tiempo de vida podría ser una medida de tiempo auténtica. Esto requiere que los dispositivos de encaminamiento conozcan de alguna manera el tiempo transcurrido desde que el datagrama o un fragmento cruzó por última vez un dispositivo de encaminamiento, para conocer cuánto tiene que decrementar el campo de tiempo de vida. Esto requeriría algún mecanismo global de sincronización. La ventaja de usar una medida real de tiempo es que se puede utilizar en el algoritmo de reensamblado descrito a continuación.

Fragmentación y reensamblado

Las redes individuales en un conjunto de redes pueden especificar tamaños máximos de paquetes diferentes. Sería ineficiente e inmanejable tratar de imponer un tamaño de paquete uniforme a través de las redes. Así, ocurre que los dispositivos de encaminamiento pueden necesitar fragmentar

los datagramas de entrada en unidades más pequeñas, llamadas segmentos o fragmentos, antes de transmitirlos en la red siguiente.

Si los datagramas se pueden fragmentar (quizá más de una vez) durante sus viajes, la cuestión que surge es dónde se deben reensamblar. La solución más fácil es realizar el reensamblado solamente en el destino. La principal desventaja de este método es que los fragmentos sólo se pueden hacer más pequeños a medida que los datos se mueven a través del conjunto de redes. Esto puede perjudicar la eficiencia de algunas redes. Por otra parte, si los dispositivos de encaminamiento intermedios pueden reensamblar, aparecen las siguientes desventajas:

1. Se requieren grandes memorias temporales en los dispositivos de encaminamiento y existe el riesgo de que todo el espacio de memoria temporal se use para almacenar datagramas parciales.

2. Todos los fragmentos de un datagrama deben pasar a través del mismo dispositivo de encaminamiento de salida. Esto imposibilita el uso del encaminamiento dinámico.

En IP, los fragmentos de los datagramas se reensamblan en el sistema final destino. La técnica de fragmentación de IP usa los siguientes campos en la cabecera IP:

- Identificador de la unidad de datos (ID).
- Longitud de los datos.
- Desplazamiento.
- Indicador de más datos.

El *ID* es un medio de identificar de forma única un datagrama originado en el sistema final. En IP, el *ID* consta de las direcciones fuente y destino, un identificador del protocolo que genera los datos (por ejemplo, TCP) y una identificación suministrada por el protocolo. La *longitud de los datos* indica la longitud del campo de datos de usuario, expresado en octetos, y el campo *desplazamiento* es la posición de un fragmento de los datos de usuario en el campo de datos en el datagrama original, en múltiplos de 64 bits.

El sistema final origen crea un datagrama con una longitud de datos igual a la longitud entera del campo de datos, con *desplazamiento* = 0 y el indicador de *más datos* establecido a 0 (falso). Para fragmentar un datagrama grande en dos piezas, un módulo IP en un dispositivo de encaminamiento realiza las siguientes tareas:

1. Crea dos nuevos datagramas y copia los campos de la cabecera del datagrama original en los datagramas nuevos.

2. Divide el campo de datos de usuario en dos porciones aproximadamente iguales con límites de 64 bits, situando una porción en cada datagrama nuevo. La primera porción debe ser un múltiplo de 64 bits (8 octetos).

3. Establece la *longitud de datos* del primer datagrama a la longitud de los datos insertados y establece a 1 (cierto) el indicador de *más datos*. El campo *desplazamiento* no se cambia.

4. Establece la *longitud de datos* del segundo datagrama a la longitud de los datos insertados, y añade la longitud de la primera porción de datos dividida por 8 al campo *desplazamiento*. El indicador de *más datos* permanece igual.

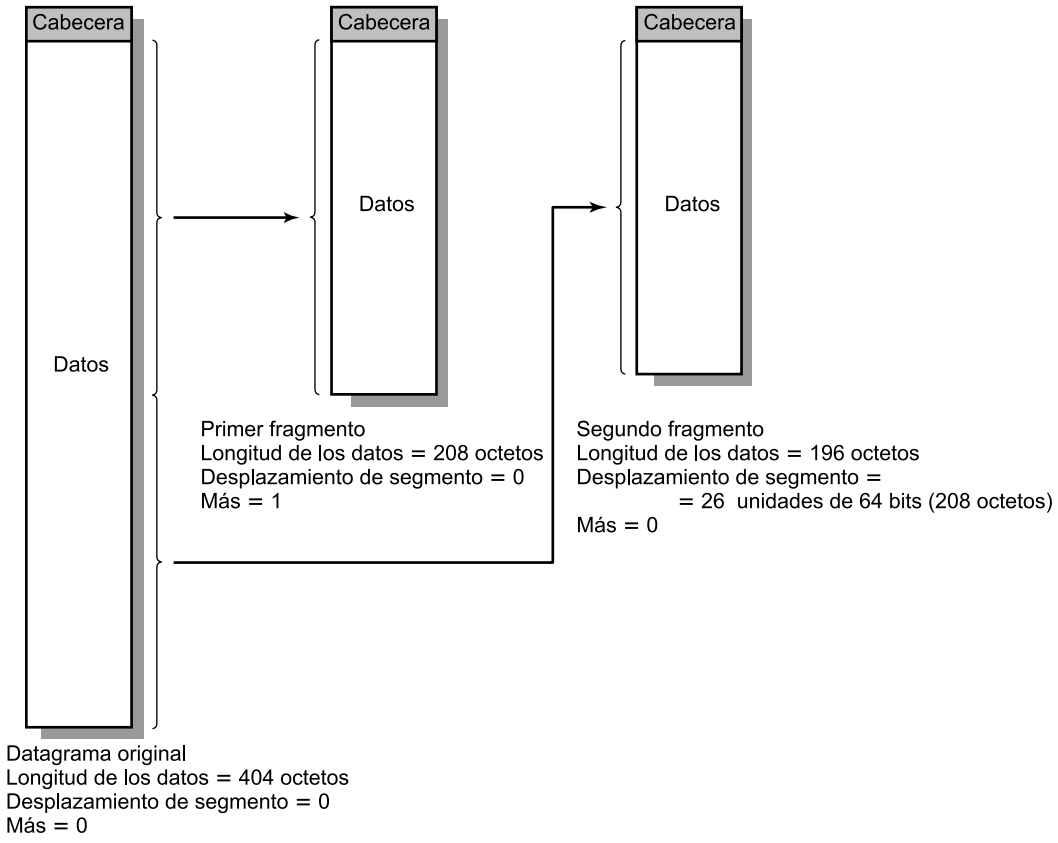


Figura 18.5. Ejemplo de fragmentación.

La Figura 18.5 muestra un ejemplo. El procedimiento se puede generalizar fácilmente a una división de *n*-caminos.

Para reensamblar un datagrama debe haber suficiente espacio de memoria temporal en el momento de reensamblar. Conforme los fragmentos con el mismo ID llegan, se insertan los campos de datos en la posición correcta en la memoria temporal hasta que el campo datos entero se reensambla, lo que se consigue cuando existe un conjunto contiguo de datos comenzando con un *desplazamiento* de cero y terminando con datos de un segmento con el indicador de *más datos* puesto a falso.

Una eventualidad con la que hay que enfrentarse es que uno o más fragmentos no hayan llegado: el servicio IP no garantiza la entrega. Se necesitan algunos métodos para decidir abandonar una tentativa de reensamblado con objeto de liberar espacio de memoria temporal. Comúnmente se utilizan dos técnicas. La primera asigna un tiempo de vida de reensamblado al primer segmento que llega. Éste se regula con un reloj en tiempo real local asignado por la función de reensamblado y decrementado mientras los fragmentos del datagrama original se van almacenando en la memoria temporal. Si el tiempo expira antes de completar el reensamblado, los fragmentos recibidos se descartan. Una segunda técnica consiste en hacer uso del tiempo de vida del datagrama, que es parte de la cabecera de cada uno de los fragmentos entrantes. El campo de vida es decrementado por la función de reensamblado. Como con la primera técnica, si el tiempo de vida expira antes de completar el reensamblado, los fragmentos recibidos se descartan.

Control de errores

El sistema de interconexión entre redes no garantiza la distribución satisfactoria de cada datagrama. Cuando un dispositivo de encaminamiento descarta un datagrama, éste debería intentar devolver alguna información al origen, si es posible. La entidad origen que usa el protocolo Internet puede emplear esta información para modificar su estrategia de transmisión y notificarlo a las capas superiores. Para informar que un datagrama específico ha sido descartado, se necesita algún medio de identificar datagramas.

Los datagramas se pueden descartar por una serie de razones, incluyendo la expiración del tiempo de vida, la existencia de congestión y de error en la suma de comprobación. En este último caso, no es posible realizar una notificación, ya que el campo de la dirección fuente puede haber sido dañado.

Control de flujo

El control de flujo en la interconexión permite a los dispositivos de encaminamiento y/o las estaciones receptoras limitar la razón a la cual se reciben los datos. Para un servicio no orientado a conexión como el que estamos describiendo, los mecanismos de control de flujo son limitados. La mejor aproximación parece ser enviar paquetes de control de flujo, solicitando una reducción del flujo de datos a otros dispositivos de encaminamiento y a las estaciones fuente. Se verá un ejemplo de esta situación con ICMP, que se discutirá en la sección siguiente.

18.4. EL PROTOCOLO INTERNET

En esta sección se examina la versión 4 de IP, definida oficialmente en el RFC 791. Aunque la intención es que IPv6 reemplace a IPv4, éste es actualmente el estándar IP utilizado en las redes TCP/IP.

El protocolo Internet (IP) es parte del conjunto de protocolos TCP/IP y es el protocolo de interconexión de redes más utilizado. Como con cualquier protocolo estándar, IP se especifica en dos partes:

- La interfaz con la capa superior (por ejemplo, TCP), especificando los servicios que proporciona IP.
- El formato real del protocolo y los mecanismos asociados.

En esta sección se examinan primero los servicios de IP y después el protocolo IP. A esto seguirá una discusión del formato de las direcciones IP. Finalmente, se describe el protocolo de mensajes de control de Internet (ICMP, *Internet Control Message Protocol*), que es una parte integral de IP.

SERVICIOS IP

Los servicios a proporcionar entre las capas de protocolos adyacentes (por ejemplo, entre IP y TCP) se expresan en términos de primitivas y parámetros. Una primitiva especifica la función que se va a ofrecer y los parámetros se utilizan para pasar datos e información de control. La forma real de una primitiva depende de la implementación. Un ejemplo es una llamada a subrutina.

IP proporciona dos primitivas de servicio en la interfaz con la capa superior. La primitiva *Send* (envío) se utiliza para solicitar la transmisión de una unidad de datos. La primitiva *Deliver* (entrega)

utiliza IP para notificar a un usuario la llegada de una unidad de datos. Los parámetros asociados a estas dos primitivas son los siguientes:

- **Dirección origen:** dirección global de red de la entidad IP que envía la unidad de datos.
- **Dirección destino:** dirección global de red de la entidad IP de destino.
- **Protocolo:** entidad de protocolo receptor (un usuario IP, como por ejemplo TCP))
- **Indicadores del tipo de servicio:** utilizado para especificar el tratamiento de la unidad de datos en su transmisión a través de los componentes de las redes.
- **Identificador:** utilizado en combinación con las direcciones origen y destino y el protocolo usuario para identificar de una forma única a la unidad de datos. Este parámetro se necesita para reensamblar e informar de errores.
- **Indicador de no fragmentación:** indica si IP puede fragmentar los datos para realizar el transporte.
- **Tiempo de vida:** medido en segundos.
- **Longitud de los datos:** longitud de los datos que se transmiten.
- **Datos de opción:** opciones solicitadas por el usuario IP.
- **Datos:** datos de usuario que se van a transmitir.

Hay que indicar que los parámetros *identificador*, *indicador de no fragmentación* y *tiempo de vida* se encuentran presentes en la primitiva *Send* pero no lo están en la primitiva *Deliver*. Estos tres parámetros proporcionan instrucciones a IP que no son de la incumbencia del usuario IP destino.

El parámetro de *opciones* permite futuras extensiones y la inclusión de parámetros que normalmente no se invocan. Las opciones actualmente definidas son:

- **Seguridad:** permite que se incorpore una etiqueta de seguridad al datagrama.
- **Encaminamiento en el origen:** constituye una lista secuencial de direcciones de dispositivos de encaminamiento que especifica la ruta a seguir. El encaminamiento puede ser estricto (sólo los dispositivos de encaminamiento identificados pueden ser visitados) o débil (pueden visitarse otros dispositivos de encaminamiento intermedios).
- **Registro de la ruta:** se reserva un campo para registrar la secuencia de dispositivos de encaminamiento visitados por el datagrama.
- **Identificación de la secuencia:** identifica recursos reservados utilizados para un servicio de secuencia. Este servicio proporciona un tratamiento especial del tráfico volátil periódico (por ejemplo, voz).
- **Marcas de tiempo:** la entidad IP origen y algunos o todos los dispositivos de encaminamiento intermedios incorporan una marca temporal (con una precisión de milisegundos) a las unidades de datos conforme van pasando por ellos.

PROTOCOLO IP

El protocolo entre entidades IP se describe mejor mediante la referencia al formato del datagrama IP mostrado en la Figura 18.6. Los campos son los siguientes:

- **Versión (4 bits):** indica el número de la versión del protocolo, para permitir la evolución del mismo; el valor es 4.

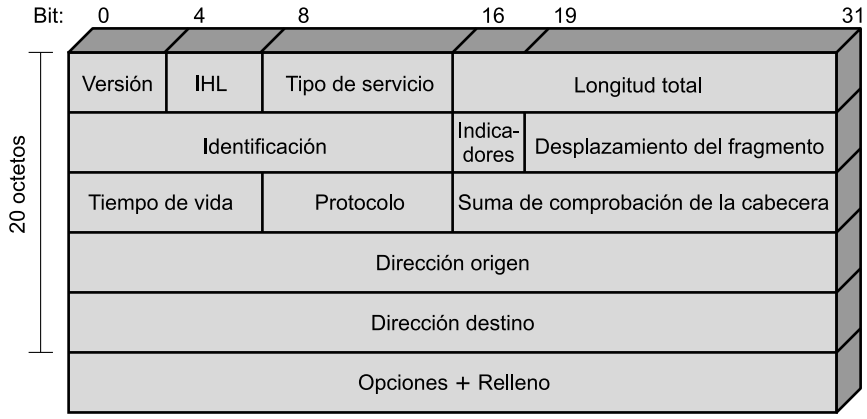


Figura 18.6. Cabecera IPv4.

- **Longitud de la cabecera Internet (IHL, *Internet Header Length*) (4 bits):** longitud de la cabecera expresada en palabras de 32 bits. El valor mínimo es de cinco, correspondiente a una longitud de la cabecera mínima de 20 octetos.
- **Tipo de servicio (8 bits):** especifica los parámetros de fiabilidad, prioridad, retardo y rendimiento. Este campo se utiliza muy raramente; su interpretación ha sido sustituida recientemente. Los primeros 6 bits del campo son denominados ahora campo de servicios diferenciados (DS, *Differentiated Services*), que se discuten en el Capítulo 19. Los 2 bits restantes están reservados para un campo de notificación explícita de congestión (ECN), actualmente en fase de estandarización. El campo ECN proporciona una señalización explícita de congestión de una manera similar a la discutida para retransmisión de tramas (*véase* Sección 13.5).
- **Longitud total (16 bits):** longitud total del datagrama, en octetos.
- **Identificador (16 bits):** un número de secuencia que, junto a la dirección origen y destino y el protocolo usuario, se utiliza para identificar de forma única un datagrama. Por tanto, el identificador debe ser único para la dirección origen del datagrama, la dirección destino y el protocolo usuario durante el tiempo en el que el datagrama permanece en la red.
- **Indicadores (3 bits):** solamente dos de estos tres bits están actualmente definidos. El bit de «más datos» se utiliza para la fragmentación y el reensamblado como se ha expuesto previamente. El bit de «no fragmentación» prohíbe la fragmentación cuando es 1. Este bit puede ser útil si se conoce que el destino no tiene capacidad de reensamblar fragmentos. Sin embargo, si este bit vale 1, el datagrama se descartará si se excede el tamaño máximo de una red en la ruta. Por tanto, cuando el bit vale 1, es aconsejable utilizar encaminamiento desde el origen para evitar redes con tamaño de paquete máximos pequeños.
- **Desplazamiento del fragmento (13 bits):** indica el lugar donde se sitúa el fragmento dentro del datagrama original, medido en unidades de 64 bits. Esto implica que todos los fragmentos excepto el último contienen un campo de datos con una longitud múltiplo de 64 bits.
- **Tiempo de vida (8 bits):** especifica cuánto tiempo, en segundos, se le permite a un datagrama permanecer en la red. Cada dispositivo de encaminamiento que procesa el datagrama debe decrementar este campo al menos en una unidad, de forma que el tiempo de vida es de alguna forma similar a una cuenta de saltos.

- **Protocolo (8 bits):** identifica el protocolo de la capa de red inmediatamente superior que va a recibir el campo de datos en el destino; así, este campo sirve para identificar el siguiente tipo de cabecera presente en el paquete después de la cabecera IP.
- **Suma de comprobación de la cabecera (16 bits):** un código de detección de errores aplicado solamente a la cabecera. Ya que algunos campos de la cabecera pueden cambiar durante el viaje (por ejemplo, el tiempo de vida y los campos relacionados con la segmentación), este valor se verifica y recalcula en cada dispositivo de encaminamiento. El campo suma de comprobación es el complemento a uno de la suma complemento a uno de todas las palabras de 16 bits en la cabecera. Por motivos de cálculo, este campo se inicializa a sí mismo a un valor de todo cero[3].
- **Dirección de origen (32 bits):** codificada para permitir una asignación variable de bits para especificar la red y el sistema final conectado a la red especificada, como se discute posteriormente.
- **Dirección destino (32 bits):** igual que el campo anterior.
- **Opciones (variable):** contiene las opciones solicitadas por el usuario que envía los datos.
- **Relleno (variable):** se usa para asegurar que la cabecera del datagrama tiene una longitud múltiplo de 32 bits.
- **Datos (variable):** el campo de datos debe tener una longitud múltiplo de 8 bits. La máxima longitud de un datagrama (campo de datos más cabecera) es de 65.535 octetos.

Debería quedar claro cómo se traducen los servicios IP especificados en las primitivas *Send* y *Deliver* en los campos del datagrama IP.

DIRECCIONES IP

Los campos dirección origen y destino en la cabecera IP contienen cada uno una dirección internet global de 32 bits que, generalmente, consta de un identificador de red y un identificador de computador.

Clases de red

La dirección está codificada para permitir una asignación variable de bits para especificar la red y el computador, como se muestra en la Figura 18.7. Este esquema de codificación proporciona flexibilidad al asignar las direcciones a los computadores y permite una mezcla de tamaños de red en un conjunto de redes. Existen tres clases principales de redes que se pueden asociar a las siguientes condiciones:

- **Clase A:** pocas redes, cada una con muchos computadores.
- **Clase B:** un número medio de redes, cada una con un número medio de computadores.
- **Clase C:** muchas redes, cada una con pocos computadores.

En un entorno particular, podría ser mejor utilizar todas las direcciones de una misma clase. Por ejemplo, en un conjunto de redes de una entidad, consistente en un gran número de redes de

[3] Se puede encontrar un estudio acerca de esta suma de comprobación en un documento de apoyo ubicado en el sitio web de este libro.

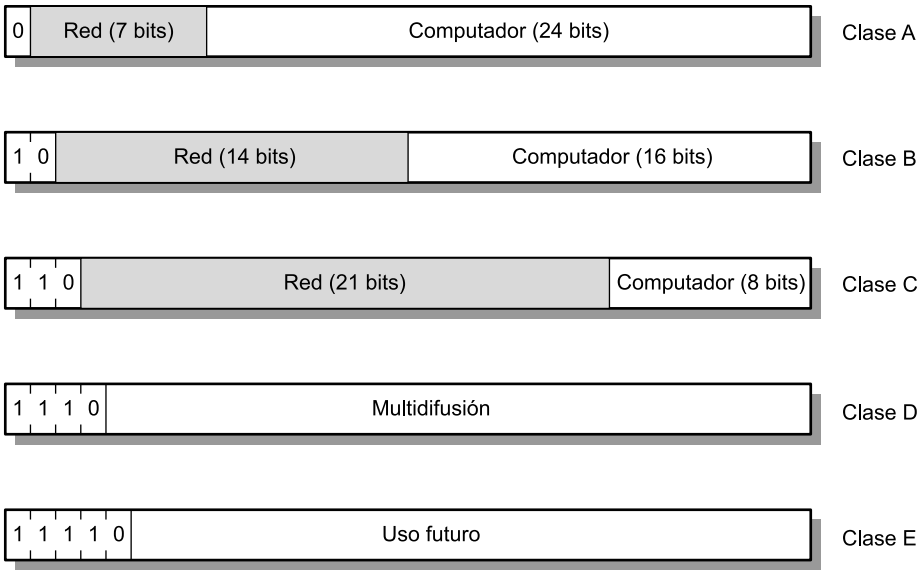


Figura 18.7. Formatos de dirección IP.

área local departamentales, podría ser necesario usar direcciones de clase C exclusivamente. Sin embargo, el formato de las direcciones es tal que es posible mezclar las tres clases de direcciones en el mismo conjunto de redes; esto es lo que se hace en el caso de la misma Internet. En el caso de un conjunto de redes formado por pocas redes grandes, muchas redes pequeñas y algunas redes de tamaño mediano, es apropiado utilizar una mezcla de clases de direcciones.

Las direcciones IP se escriben normalmente en lo que se llama *notación punto decimal*, utilizando un número decimal para representar cada uno de los octetos de la dirección de 32 bits. Por ejemplo, la dirección IP 11000000 11100100 00010001 00111001 se escribe como 192.228.17.57.

Obsérvese que todas las direcciones de red de clase A empiezan con un 0 binario. Las direcciones de red con el primer octeto puesto a 0 (en binario 00000000) o que sea 127 (en binario 01111111) están reservadas. Por tanto, existen 126 números de red potenciales de clase A en los cuales su primer octeto en formato punto decimal está en el rango de 1 a 126. Las direcciones de red de clase B comienzan con un número binario 10, de forma que su primer número decimal está entre 128 y 191 (en binario entre 10000000 y 10111111). El segundo octeto también forma parte de la dirección de clase B, de forma que existen $2^{14} = 16.384$ direcciones de clase B. Para las direcciones de clase C, el primer número decimal va de 192 a 223 (de 11000000 a 11011111). El número total de direcciones de clase C es de $2^{21} = 2.097.152$.

Subredes y máscaras de subred

El concepto de subred fue introducido como una solución para el siguiente problema. Considere un conjunto de redes que incluye una o más WAN y un determinado número de sitios, cada uno de ellos con un determinado número de LAN. Nos gustaría tener una complejidad arbitraria de estructuras de LAN interconectadas dentro de la organización, aislando al resto del conjunto de redes frente a un crecimiento explosivo en el número de redes y la complejidad en el encaminamiento. Una solución a este problema es asignar a todas las LAN en un sitio un único número de red.

Desde el punto de vista del resto del conjunto de redes, existe una única red en ese sitio, lo cual simplifica el direccionamiento y el encaminamiento. Para permitir que los dispositivos de encaminamiento internos al sitio funcionen correctamente, a cada LAN se le asigna un número de subred. La parte *computador* en la dirección internet se divide en un número de subred y un número de computador para acomodar este nuevo nivel de direccionamiento.

Dentro de una red dividida en subredes, los dispositivos de encaminamiento locales deben encaminar sobre la base de un número de red extendido consistente en la porción de *red* de la dirección IP y el número de subred. Las posiciones a nivel de bit que contienen este número de red extendido se indican mediante la máscara de dirección. El uso de esta máscara de dirección permite a un computador determinar si un datagrama de salida va destinado a otro computador en la misma LAN (entonces se envía directamente) o a otra LAN (se envía a un dispositivo de encaminamiento). Se supone que se utiliza algún otro medio (por ejemplo, mediante la configuración manual) para crear las máscaras de dirección y darlas a conocer a los dispositivos de encaminamiento locales.

La Tabla 18.3a muestra los cálculos que se realizan con la utilización de una máscara de subred. Obsérvese que el efecto de la máscara de subred es borrar la parte del campo de computador que indica el computador real en una subred. Lo que permanece es el número de red y el número de subred. La Figura 18.8 muestra un ejemplo de utilización de subredes. La figura muestra un complejo local consistente en tres LAN y dos dispositivos de encaminamiento. Para el resto del conjunto de redes este complejo es una red única con una dirección de clase C de la forma 192.228.17.*x*, donde los tres octetos más a la izquierda son el número de red y el octeto más a la derecha contiene un número de computador *x*. Ambos dispositivos de encaminamiento R1 y R2 se

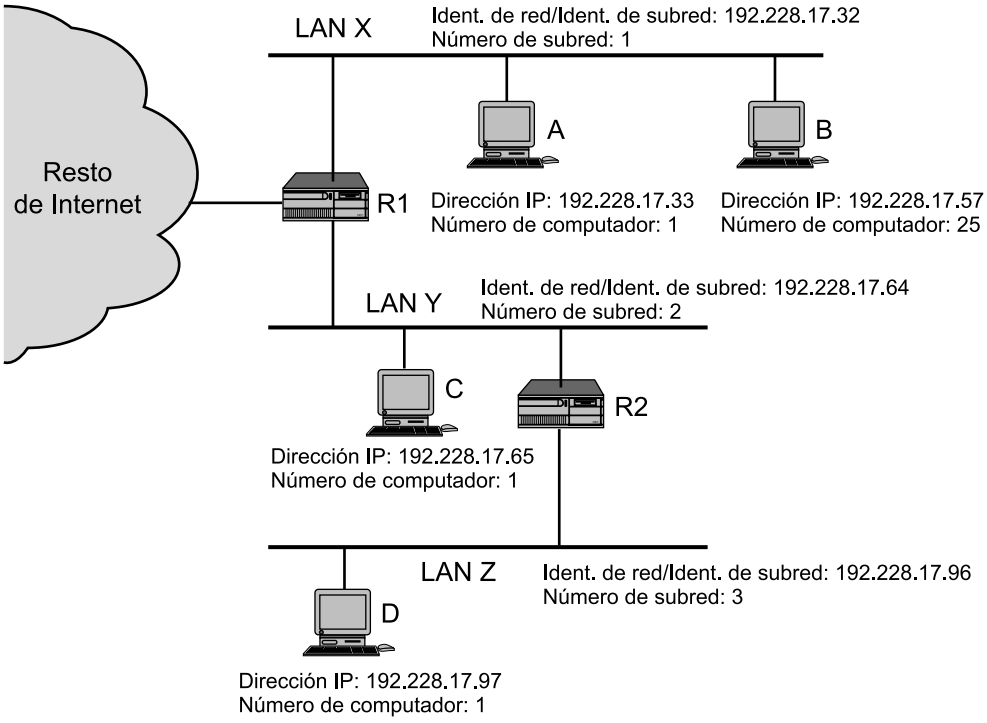


Figura 18.8. Ejemplo de utilización de subredes.

Tabla 18.3. Direcciones IP y máscaras de subred [STEI95].

(a) Representaciones punto decimal y binaria de las direcciones IP y las máscaras de subred

	Representación binaria	**Punto decimal**
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.11100000	255.255.255.224
Operación AND bit-a-bit de la dirección y la máscara (número de red/subred resultante)	11000000.11100100.00010001.00100000	192.228.17.32
Número de subred	11000000.11100100.00010001.001	1
Número de computador	00000000.00000000.00000000.00011001	25

(b) Máscaras de subred por defecto

	Representación binaria	**Punto decimal**
Máscara de clase A por defecto	11111111.00000000.00000000.00000000	255.0.0.0
Ejemplo de máscara de clase A	11111111.11000000.00000000.00000000	255.192.0.0
Máscara de clase B por defecto	11111111.11111111.00000000.00000000	255.255.0.0
Ejemplo de máscara de clase B	11111111.11111111.11111000.00000000	255.255.248.0
Máscara de clase C por defecto	11111111.11111111.11111111.00000000	255.255.255.0
Ejemplo de máscara de clase C	11111111.11111111.11111111.11111100	255.255.255.252

configuran con una máscara de subred con el valor 255.255.255.224 (*véase* la Tabla 18.3a). Por ejemplo, si un datagrama con una dirección destino 192.228.17.57 llega a R1 desde el resto del conjunto de redes o desde la LAN Y, R1 aplica la máscara de subred para determinar que esta dirección hace referencia a una dirección de la subred 1, la cual es la LAN X, y si es así enviarlo a la LAN X. De forma similar, si llega un datagrama con esa dirección destino a R2 desde la LAN Z, R2 aplica la máscara y determina a partir de su base de datos que el datagrama destinado a la subred 1 se debe enviar a R1. Los computadores también utilizan la máscara de subred para tomar decisiones de encaminamiento.

La máscara de subred por defecto para una clase de direcciones dada es una máscara nula (Tabla 18.3b), que produce el mismo número de red y de computador que en el caso de una dirección sin subredes.

PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET (ICMP)

El estándar IP especifica que una implementación que cumpla las especificaciones del protocolo debe también implementar ICMP (RFC 792). ICMP proporciona un medio para transferir mensajes desde los dispositivos de encaminamiento y otros computadores a un computador. En esencia, ICMP proporciona información de realimentación sobre problemas del entorno de la comunicación. Algunas situaciones donde se utiliza son: cuando un datagrama no puede alcanzar su destino, cuando el dispositivo de encaminamiento no tiene la capacidad de almacenar temporalmente para

reenviar el datagrama y cuando el dispositivo de encaminamiento indica a una estación que envíe el tráfico por una ruta más corta. En la mayoría de los casos, el mensaje ICMP se envía en respuesta a un datagrama, bien por un dispositivo de encaminamiento en el camino del datagrama o por el computador destino deseado.

Aunque ICMP está, a todos los efectos, en el mismo nivel que IP en el conjunto de protocolos TCP/IP, es un usuario de IP. Cuando se construye un mensaje ICMP, éste se pasa a IP, que encapsula el mensaje con una cabecera IP y después transmite el datagrama resultante de la forma habitual. Ya que los mensajes ICMP se transmiten en datagramas IP, no se garantiza su entrega y su uso no se puede considerar fiable.

La Figura 18.9 muestra el formato de varios tipos de mensajes ICMP. Todos los mensajes ICMP empiezan con una cabecera de 64 bits que consta de los siguientes campos:

- **Tipo (8 bits):** especifica el tipo de mensaje ICMP.
- **Código (8 bits):** se usa para especificar parámetros del mensaje que se pueden codificar en uno o unos pocos bits.
- **Suma de comprobación (16 bits):** suma de comprobación del mensaje ICMP entero. Se utiliza el mismo algoritmo de suma de comprobación que en IP.
- **Parámetros (32 bits):** se usa para especificar parámetros más largos.

A estos campos les siguen generalmente campos de información adicional que especifican aún más el contenido del mensaje.

En aquellos casos en los que un mensaje ICMP se refiere a un datagrama previo, el campo de información incluye la cabecera IP entera más los primeros 64 bits del campo de datos del datagrama original. Esto permite al computador origen emparejar el mensaje ICMP que llega con el

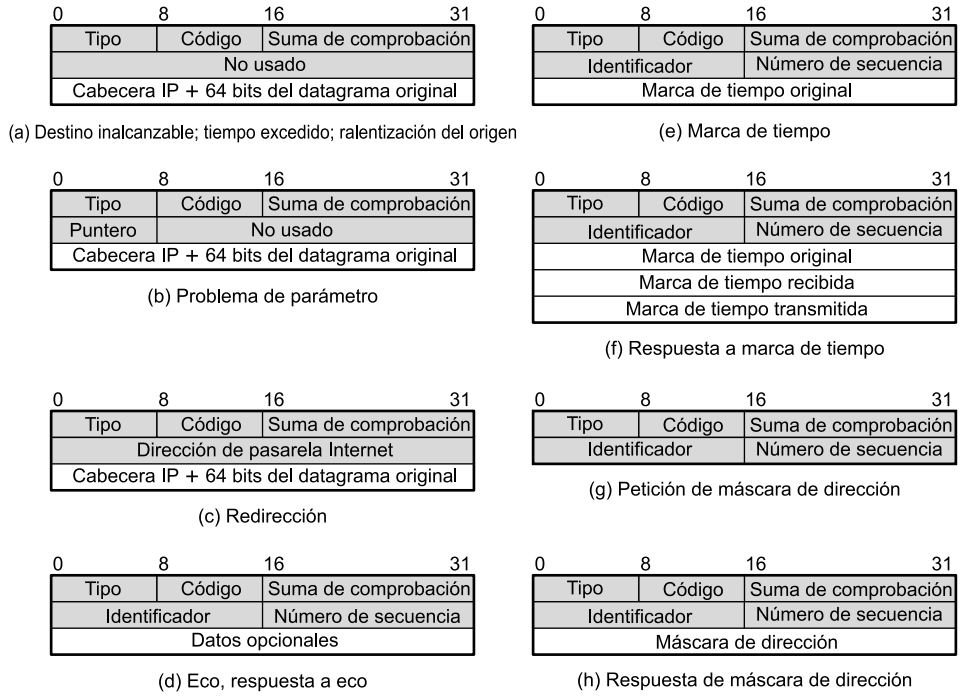


Figura 18.9. Formatos de mensajes ICMP.

datagrama anterior. La razón de incorporar los primeros 64 bits del campo de datos es que permite al módulo IP en el computador determinar qué protocolo o protocolos del nivel superior estaban implicados. En particular, los primeros 64 bits incluirían una porción de la cabecera TCP u otra cabecera del nivel de transporte.

El mensaje **destino inalcanzable** cubre un cierto número de situaciones. Un dispositivo de encaminamiento puede devolver este mensaje si no sabe cómo alcanzar la red destino. En algunas redes, un dispositivo de encaminamiento conectado a una de estas redes puede ser capaz de determinar si un computador es inalcanzable y devolver este tipo de mensaje. El propio computador de destino puede devolver este mensaje si el protocolo de usuario o algún punto de acceso al servicio de un nivel superior no están alcanzables. Esto puede ocurrir si el correspondiente campo en la cabecera IP no tiene el valor correcto. Si el datagrama especifica una ruta dada por la fuente que no se puede usar, se devolverá un mensaje. Finalmente, si un dispositivo de encaminamiento debe fragmentar un datagrama pero el indicador de no fragmentación está establecido, se devuelve también el mensaje «destino inalcanzable».

Un dispositivo de encaminamiento devolverá el mensaje **tiempo excedido** si el tiempo de vida del datagrama ha expirado. Un computador enviará este mensaje si no puede completar el reensamblado dentro del margen de tiempo disponible.

Un error sintáctico o semántico en la cabecera IP causará que un dispositivo de encaminamiento o un computador devuelvan un mensaje de **problema de parámetro**. Por ejemplo, puede existir un argumento incorrecto en una opción. El campo parámetro de la respuesta contiene un puntero al octeto en la cabecera original donde se detectó el error.

El mensaje de **ralentización del origen** proporciona una forma rudimentaria de control de flujo. Este mensaje lo pueden enviar tanto un dispositivo de encaminamiento como un computador destino a un computador origen solicitando que reduzca la tasa a la que envía el tráfico al destino. Cuando se recibe este tipo de mensaje, un computador origen debe disminuir la tasa de datos a la que envía el tráfico al destino especificado hasta que no reciba más mensajes de ralentización del origen. El mensaje de ralentización del origen lo puede generar tanto un dispositivo de encaminamiento como un computador que deba descartar datagramas debido a que su memoria temporal está llena. En este caso, el dispositivo de encaminamiento o el computador enviará un mensaje de ralentización del origen por cada datagrama que se descarta. Además, un sistema se puede anticipar a la congestión y enviar este tipo de mensaje cuando su memoria esté a punto de llegar a su capacidad máxima. En ese caso, el datagrama referido en el mensaje de ralentización del origen podrá ser entregado correctamente. Así, la recepción de un mensaje de ralentización no implica la entrega o la no entrega del datagrama correspondiente.

Un dispositivo de encaminamiento envía un mensaje de **redirección** a un computador conectado directamente a un dispositivo de encaminamiento para informarle de una ruta mejor para un destino particular. A continuación se da un ejemplo de su uso utilizando la Figura 18.8. El dispositivo de encaminamiento R1 recibe un datagrama del computador C en la red Y a la que está conectado R1. El dispositivo de encaminamiento R1 comprueba su tabla de encaminamiento y obtiene la dirección del siguiente dispositivo de encaminamiento, R2, en la ruta del datagrama a la red destino, Z. Puesto que R2 y el computador identificado por la dirección internet origen del datagrama están en la misma red, R1 envía un mensaje de redirección al computador C. Este mensaje informa al computador para que envíe su tráfico para la red Z directamente al dispositivo de encaminamiento R2, ya que éste es el camino más corto al destino. El dispositivo de encaminamiento envía el datagrama original a su destino (vía R2). La dirección de R2 se encuentra en el campo de parámetros del mensaje de redirección.

Los mensajes **eco** y **respuesta a eco** proporcionan un mecanismo para comprobar que la comunicación entre dos entidades es posible. El receptor de un mensaje de eco está obligado a devolver el mensaje en un mensaje de respuesta a eco. Al mensaje de eco se le asocia un identificador y un número de secuencia que coinciden con los de paquete de respuesta a eco. El identificador se puede utilizar como un punto de acceso al servicio, para identificar una sesión particular, y el número de secuencia se puede incrementar en cada petición de eco enviada.

Los mensajes **marca de tiempo** y **respuesta a marca de tiempo** proporcionan un mecanismo para muestrear las características en cuanto a retardo del conjunto de redes. El emisor de un mensaje marca de tiempo puede incluir un identificador y un número de secuencia en el campo parámetros e incluye el tiempo en el cual se envió el mensaje (marca de tiempo original). El receptor registra, en el mensaje respuesta, el tiempo en que recibió el mensaje y el tiempo en que transmitió el mensaje de respuesta. Si el mensaje marca de tiempo se envía usando un encaminamiento en el origen estricto, se pueden determinar las características de retardo de una ruta particular.

Los mensajes **petición de máscara de dirección** y **respuesta a máscara de dirección** son útiles en un entorno que incluya subredes. Los mensajes de petición y respuesta de máscara de dirección permiten a un computador conocer la máscara de dirección usada en la LAN a la que está conectado. El computador emite por difusión un mensaje de petición de máscara de dirección en la LAN. El dispositivo de encaminamiento en la LAN responde con un mensaje de respuesta a máscara de red que contiene la máscara de dirección.

18.5. IPv6

El Protocolo Internet (IP) ha sido el fundamento de Internet y virtualmente de todas las redes privadas de múltiples proveedores. Este protocolo está alcanzando el fin de su vida útil y se ha definido un nuevo protocolo conocido como IPv6 (IP versión 6) para, en última instancia, reemplazar a IP[4].

En primer lugar, examinaremos la motivación para desarrollar una nueva versión de IP y después analizaremos algunos de sus detalles.

IP DE NUEVA GENERACIÓN

El motivo que ha conducido a la adopción de una nueva versión ha sido la limitación impuesta por el campo de dirección de 32 bits en IPv4. Con un campo de dirección de 32 bits, en principio es posible asignar 2^{32} direcciones diferentes, alrededor de 4.000 millones de direcciones posibles. Se podría pensar que este número de direcciones era más que adecuado para satisfacer las necesidades en Internet. Sin embargo, a finales de la década de los ochenta se percibió que habría un problema y este problema empezó a manifestarse a comienzos de la década de los noventa. Algunas de las razones por las que es inadecuado utilizar estas direcciones de 32 bits son las siguientes:

- La estructura en dos niveles de la dirección IP (número de red, número de computador) es conveniente pero también es una forma poco económica de utilizar el espacio de direcciones. Una vez que se le asigna un número de red a una red, todos los números de computador de

[4] Se podría pensar que se han saltado varias versiones en este libro. La versión en uso de IP es actualmente la versión 4; las versiones previas de IP (de la 1 a la 3) fueron sucesivamente definidas y sustituidas hasta alcanzar IPv4. La versión 5 es el número asignado al protocolo de flujo (*stream protocol*), un protocolo de la capa internet orientado a conexión. De aquí el uso de la etiqueta versión 6.

ese número de red se asignan a esa red. El espacio de direcciones para esa red podría estar poco usado, pero en lo que concierne a la efectividad del espacio de direcciones, si se usa un número de red entonces se consumen todas las direcciones dentro de la red.

- El modelo de direccionamiento de IP requiere que se le asigne un número de red único a cada red IP independientemente de si la red está realmente conectada a Internet.
- Las redes están proliferando rápidamente. La mayoría de las organizaciones establecen LAN múltiples, no un único sistema LAN. Las redes inalámbricas están adquiriendo un mayor protagonismo. Internet misma ha crecido explosivamente durante años.
- El uso creciente de TCP/IP en áreas nuevas producirá un crecimiento rápido en la demanda de direcciones únicas IP (por ejemplo, el uso de TCP/IP para interconectar terminales electrónicos de puntos de venta y para los receptores de televisión por cable).
- Normalmente, se asigna una dirección única a cada computador. Una disposición más flexible es permitir múltiples direcciones IP a cada computador. Esto, por supuesto, incrementa la demanda de direcciones IP.

Por tanto, la necesidad de un incremento en el espacio de direcciones ha impuesto la necesidad de una nueva versión de IP. Además, IP es un protocolo muy viejo y se han definido nuevos requisitos en las áreas de configuración de red, flexibilidad en el encaminamiento y funcionalidades para el tráfico.

En respuesta a estas necesidades, el Grupo de Trabajo de Ingeniería de Internet (IETF) emitió una solicitud de propuestas para una nueva generación de IP (IPng) en julio de 1992. Se recibieron varias propuestas y en 1994 emergió el diseño final de IPng. Uno de los hechos destacados del desarrollo fue la publicación del RFC 1752, «La recomendación para el protocolo de nueva generación de IP», publicado en enero de 1995. El RFC 1752 describe los requisitos de IPng, especifica el formato de la PDU y señala las técnicas de IPng en las áreas de direccionamiento, encaminamiento y seguridad. Existen otros documentos Internet que definen los detalles del protocolo, ahora llamado oficialmente IPv6; éstos incluyen una especificación general de IPv6 (RFC 2460), un RFC que trata sobre la estructura de direccionamiento de IPv6 (RFC 2373) y una larga lista adicional.

IPv6 incluye las siguientes mejoras sobre IPv4:

- **Un espacio de direcciones ampliado:** IPv6 utiliza direcciones de 128 bits en lugar de las direcciones de 32 bits de IPv4. Esto supone un incremento del espacio de direcciones en un factor de 2^{96}. Se ha señalado [HIND95] que esto permite espacios de direcciones del orden de 6×10^{23} por metro cuadrado de la superficie de la tierra. Incluso si la asignación de direcciones fuera muy ineficiente, este espacio de direcciones parece seguro.
- **Un mecanismo de opciones mejorado:** las opciones de IPv6 se encuentran en cabeceras opcionales separadas situadas entre la cabecera IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras opcionales no se examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete. Esto simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los paquetes IPv6 en comparación a los datagramas IPv4[5]. Esto también hace que sea más fácil incorporar opciones adicionales.
- **Autoconfiguración de direcciones:** esta capacidad proporciona una asignación dinámica de direcciones IPv6.

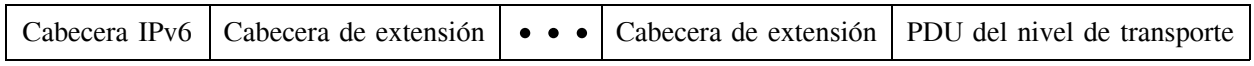
[5] La unidad de datos de protocolo para IPv6 se denomina paquete en lugar de datagrama, que es el término que se utiliza para las PDU de IPv4.

- **Aumento de la flexibilidad en el direccionamiento:** IPv6 incluye el concepto de una dirección monodifusión (*anycast*), mediante la cual un paquete se entrega sólo a un nodo seleccionado de entre un conjunto de nodos. Se mejora la escalabilidad del encaminamiento multidistribución con la incorporación de un campo de ámbito a las direcciones multidistribución.
- **Funcionalidad para la asignación de recursos:** en lugar del campo tipo de servicio de IPv4, IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el que el emisor solicita un tratamiento especial. Esto ayuda al tratamiento de tráfico especializado como el de vídeo en tiempo real.

Todas estas características se exploran en el resto de la sección, excepto las características de seguridad, que se discuten en el Capítulo 21.

ESTRUCTURA IPv6

Una unidad de datos del protocolo de IPv6 (conocida como paquete) tiene el formato general siguiente:



La única cabecera que se requiere se denomina simplemente cabecera IPv6. Ésta tiene una longitud fija de 40 octetos, comparados con los 20 octetos de la parte obligatoria de la cabecera IPv4 (*véase* Figura 18.6). Se han definido las siguientes cabeceras de extensión:

- **Cabecera de opciones salto a salto:** define opciones especiales que requieren procesamiento en cada salto.
- **Cabecera de encaminamiento:** proporciona un encaminamiento ampliado, similar al encaminamiento en el origen de IPv4.
- **Cabecera de fragmentación:** contiene información de fragmentación y reensamblado.
- **Cabecera de autenticación:** proporciona la integridad del paquete y la autenticación.
- **Cabecera de encapsulamiento de la carga de seguridad:** proporciona privacidad.
- **Cabecera de las opciones para el destino:** contiene información opcional para que sea examinada en el nodo destino.

El estándar IPv6 recomienda que, en el caso de que se usen varias cabeceras de extensión, las cabeceras IPv6 aparezcan en el siguiente orden:

1. Cabecera IPv6: obligatoria, debe aparecer siempre primero.
2. Cabecera de las opciones salto a salto.
3. Cabecera de las opciones para el destino: para opciones a procesar por el primer destino que aparece en el campo dirección IPv6 de destino y por los destinos subsecuentes indicados en la cabecera de encaminamiento.
4. Cabecera de encaminamiento.
5. Cabecera de fragmentación.
6. Cabecera de autenticación.
7. Cabecera de encapsulado de la carga de seguridad.

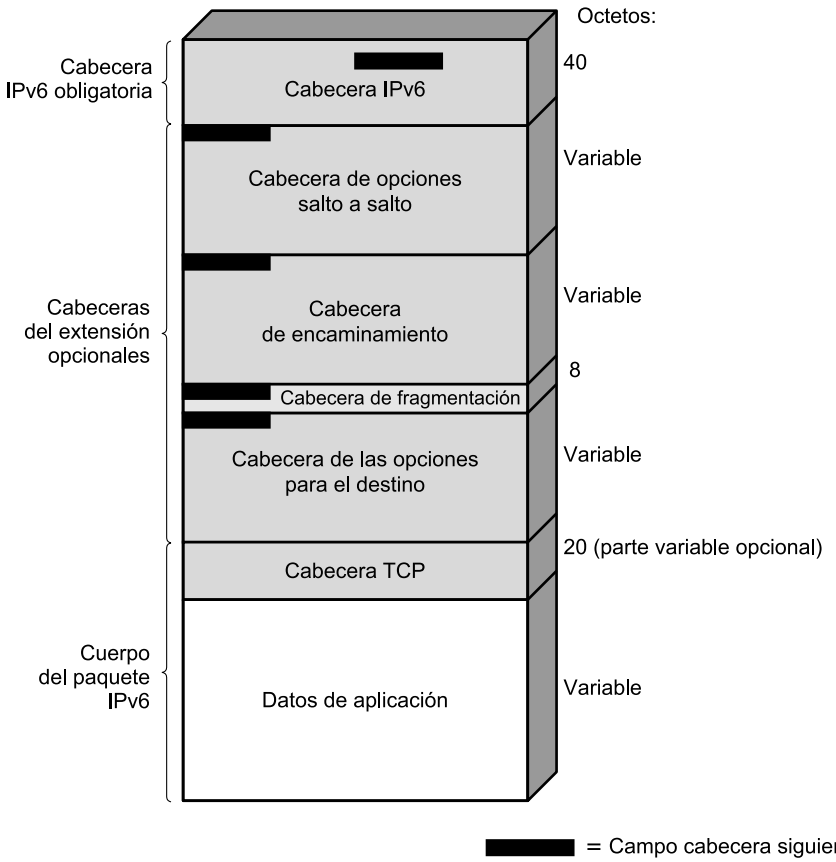


Figura 18.10. Paquete IPv6 con las cabeceras de extensión (conteniendo un segmento TCP).

8. Cabecera de opciones para el destino: para opciones a procesar por el destino final del paquete.

La Figura 18.10 muestra un ejemplo de un paquete IPv6 que incluye un ejemplar de cada cabecera, excepto aquellas relacionadas con la seguridad. Obsérvese que la cabecera IPv6 y cada cabecera de extensión incluyen el campo cabecera siguiente. Este campo identifica el tipo de cabecera que viene a continuación. Si la siguiente cabecera es de extensión, entonces este campo contiene el identificador del tipo de esa cabecera. En caso contrario, este campo contiene el identificador del protocolo de la capa superior que está usando a IPv6 (normalmente un protocolo de la capa de transporte), utilizando el mismo valor que el campo protocolo de IPv4. En la Figura 18.10, el protocolo de la capa superior es TCP; por tanto, los datos de la capa superior transportados por el paquete IPv6 constan de una cabecera TCP seguida por un bloque de datos de aplicación.

A continuación, se examina la cabecera principal de IPv6 y después se examinan cada una de las extensiones.

CABECERA IPv6

La cabecera IPv6 tiene una longitud fija de 40 octetos, que consta de los siguientes campos (*véase* Figura 18.11):

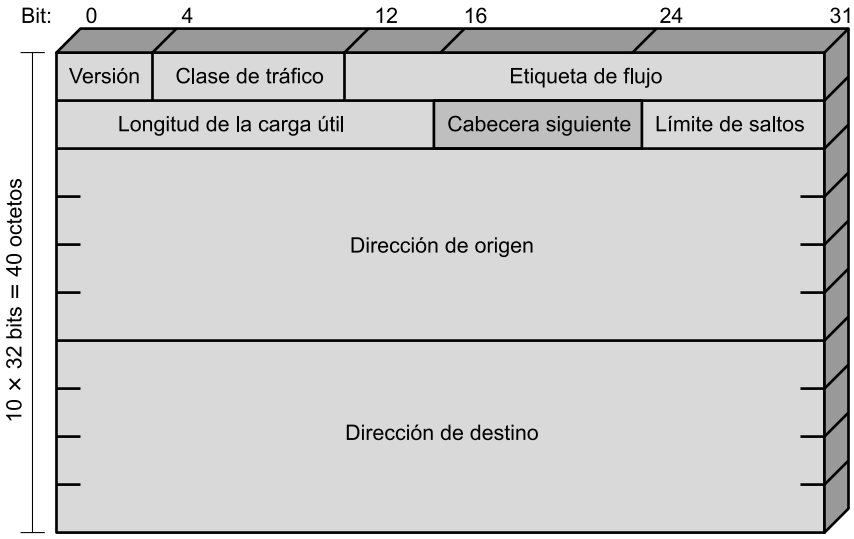


Figura 18.11. Cabecera IPv6.

- **Versión (4 bits):** número de la versión del protocolo Internet; el valor es 6.
- **Clase de tráfico (8 bits):** disponible para su uso por el nodo origen y/o los dispositivos de encaminamiento para identificar y distinguir entre clases o prioridades de paquete IPv6. Este campo se usa actualmente para los campos de ceros y ECN, como se describió para el campo tipo de servicio en IPv4.
- **Etiqueta de flujo (20 bits):** se puede utilizar por un computador para etiquetar aquellos paquetes para los que requiere un tratamiento especial en los dispositivos de encaminamiento dentro de la red; se discute después.
- **Longitud de la carga útil (16 bits):** longitud del resto del paquete IPv6 excluida la cabecera, en octetos. En otras palabras, representa la longitud de todas las cabeceras de extensión más la PDU de la capa de transporte.
- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6; se puede tratar tanto de una cabecera de extensión IPv6 como de una cabecera de la capa superior, como TCP o UDP.
- **Límite de saltos (8 bits):** el número restante de saltos permitidos para este paquete. El límite de saltos se establece por la fuente a algún valor máximo deseado y se decrementa en 1 en cada nodo que reenvía el paquete. El paquete se descarta si el límite de saltos se hace cero. Esto es una simplificación del procesamiento requerido por el campo tiempo de vida de IPv4. El consenso fue que el esfuerzo extra de contabilizar los intervalos de tiempo en IPv4 no añadía un valor significativo al protocolo. De hecho, y como regla general, los dispositivos de encaminamiento IPv4 tratan el campo tiempo de vida como un límite de saltos.
- **Dirección origen (128 bits):** dirección del productor del paquete.
- **Dirección destino (128 bits):** dirección de destino deseado del paquete. Puede que éste no sea en realidad el último destino deseado si está presente la cabecera de encaminamiento, como se explicará después.

Aunque la cabecera IPv6 es más grande que la parte obligatoria de la cabecera IPv4 (40 octetos frente a 20 octetos), contiene menos campos (8 frente a 12). Así, los dispositivos de encaminamiento tienen que hacer menos procesamiento por paquete, lo que agiliza el encaminamiento.

Clase de tráfico

El campo de clase de tráfico de 8 bits permite a una fuente identificar las características en el tratamiento de tráfico que desea cada paquete en relación con otros paquetes procedentes de la misma fuente. Al igual que ocurrió con el campo TOS (Tipo de Servicio) de IPv4, la intención original del campo clase de tráfico ha sido suplantada. Actualmente, los primeros seis bits del campo clase de tráfico se denominan campo de servicios diferenciados (DS, *Differentiated Services*), discutidos en el Capítulo 19. Los 2 bits restantes se reservan para un campo de notificación explícita de congestión (ECN, *Explicit Congestion Notification*), encontrándose actualmente en proceso de estandarización. El campo ECN proporcionará un mecanismo para señalizar explícitamente la congestión de una manera similar a la que se discutió para retransmisión de tramas (*véase* Sección 13.5).

Etiqueta de flujo

El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen particular a un destino particular (monodistribución o multidistribución) y para el que el origen desea un tratamiento especial por parte de los dispositivos de encaminamiento. Un flujo está unívocamente identificado por la combinación de una dirección origen, una dirección destino y una etiqueta de flujo de 20 bits distinta de cero. Así, todos los paquetes que van a formar parte del mismo flujo tienen asignada por el origen la misma etiqueta de flujo.

Desde el punto de vista del origen, un flujo será normalmente una secuencia de paquetes que se generan por una única aplicación en el origen y tienen los mismos requisitos del servicio de transferencia. Un flujo puede estar compuesto de una única conexión TCP o incluso de varias. Un ejemplo de este último caso es una aplicación de transferencia de ficheros, que podría tener una conexión de control y varias conexiones de datos. Una única aplicación puede generar un único flujo o varios flujos. Un ejemplo de este último caso es la conferencia multimedia, que podría tener un flujo para audio y otro para ventanas gráficas, cada una con diferentes requisitos de transmisión en términos de tasa de datos, retardo y variación del retardo.

Desde el punto de vista de los dispositivos de encaminamiento, un flujo es una secuencia de paquetes que comparten atributos que afectan a cómo deben ser tratados por el dispositivo de encaminamiento. Estos incluyen atributos de camino, asignación de recursos, requisitos sobre cómo descartar, contabilidad de paquetes transmitidos y atributos de seguridad. El dispositivo de encaminamiento puede tratar los paquetes de diferentes flujos de forma diversa, incluyendo la asignación de diferentes tamaños de memoria temporal, dando diferente precedencia en términos de reenvío y solicitando de las redes diferentes calidades de servicio.

Ninguna etiqueta de flujo tiene un significado especial. En consecuencia, el tratamiento especial que se ha de dar al flujo de paquetes se debe declarar de alguna forma. Por ejemplo, un origen podría negociar o solicitar a los dispositivos de encaminamiento un determinado tratamiento de forma anticipada por medio de un protocolo de control, o en el momento de la transmisión, mediante información insertada en alguna de las cabeceras de extensión del paquete, como puede ser en la cabecera de opciones de salto a salto. Como ejemplo de tratamiento especial que se podría solicitar están el de una calidad de servicio que sea diferente de la establecida implícitamente o alguna forma de servicio en tiempo real.

En principio, todos los requisitos de un usuario para un flujo particular se podrían definir en una cabecera de extensión incluida en todos los paquetes. Si queremos dejar el concepto de flujo abierto para incluir una gran variedad de requisitos, esta técnica de diseño daría lugar a cabeceras de paquete muy grandes. La alternativa, adoptada por IPv6, es la etiqueta de flujo, en la que los requisitos de flujo se definen antes de comenzar el flujo y se le asigna una única etiqueta. En este caso, el dispositivo de encaminamiento debe guardar la información sobre los requisitos de flujo de cada uno de los flujos.

Se aplican las siguientes reglas a las etiquetas de flujo:

1. Los computadores o dispositivos de encaminamiento que no soportan el campo de etiqueta de flujo deben poner a cero este campo cuando generan un paquete, no cambiar el campo cuando reenvían e ignorar el campo cuando reciben un paquete.
2. Todos los paquetes producidos en un origen dado con la misma etiqueta de flujo distinta de cero deben tener la misma dirección destino, dirección origen y el mismo contenido en las cabeceras de opciones salto a salto y de encaminamiento (si estas cabeceras están presentes). La intención es que un dispositivo de encaminamiento pueda decidir cómo encaminar y procesar el paquete simplemente buscando la etiqueta de flujo en una tabla, sin examinar el resto de la cabecera.
3. El origen asigna a cada flujo una etiqueta de flujo. Las etiquetas de flujo nuevas se deben elegir (pseudo)aleatoriamente y uniformemente en el rango de 1 a $2^{20} - 1$, teniendo en cuenta la restricción de que el origen no puede reutilizar una etiqueta de flujo para un flujo nuevo en el tiempo de vida del flujo existente. La etiqueta de flujo cero se reserva para indicar que no se está utilizando etiquetado en el flujo.

Este último punto requiere alguna aclaración adicional. El dispositivo de encaminamiento debe mantener, presumiblemente en algún tipo de tabla, la información sobre las características de cada flujo activo que puede pasar por él. Para que sea capaz de reenviar los paquetes eficiente y rápidamente, la búsqueda en la tabla ha de ser eficiente. Una alternativa es tener una tabla con 2^{20} (alrededor de 16 millones) elementos, uno por cada etiqueta de flujo posible; esto impone una capacidad de memoria innecesaria en el dispositivo de encaminamiento. Otra alternativa es tener un elemento en la tabla por cada flujo activo y que incluya la etiqueta de flujo, lo que requiere que el dispositivo de encaminamiento busque en la tabla entera cada vez que le llega un paquete. Esto supone una carga de procesamiento innecesaria en el dispositivo de encaminamiento. En lugar de esto, la mayoría de los diseños de dispositivos de encaminamiento utilizan frecuentemente algún tipo de enfoque basado en una tabla de dispersión (*hash*). Con este enfoque se utiliza una tabla de tamaño moderado y a cada flujo se le asigna un elemento de la tabla utilizando una función de mezcla de la etiqueta de flujo. Esta función de mezcla podría ser simplemente extraer los bits menos significativos (por ejemplo, los 8 o 10 bits más bajos) de la etiqueta de flujo o algún cálculo sencillo con los 20 bits de la etiqueta de flujo. En cualquier caso, la eficiencia del planteamiento de funciones de dispersión normalmente depende de que las etiquetas de flujo estén distribuidas uniformemente en su rango posible (de aquí el requisito número 3 indicado anteriormente).

DIRECCIONES IPv6

Las direcciones IPv6 tienen una longitud de 128 bits. Las direcciones se asignan a interfaces individuales en los nodos, no a los nodos[6]. Una única interfaz puede tener múltiples direcciones

[6] En IPv6, un *nodo* es cualquier dispositivo que implemente IPv6; esto incluye a computadores y dispositivos de encaminamiento.

únicas. Cualquiera de las direcciones asociadas a las interfaces de los nodos se puede utilizar para identificar de forma única al nodo.

La combinación de direcciones largas y direcciones múltiples por interfaz permite una eficiencia mejorada del encaminamiento con respecto a IPv4. En IPv4, generalmente las direcciones no tienen una estructura que ayude al encaminamiento y, por tanto, un dispositivo de encaminamiento necesita mantener una gran tabla con rutas de encaminamiento. Una dirección internet más grande permite agrupar las direcciones por jerarquías de red, por proveedores de acceso, por proximidad geográfica, por institución, etc. Estas agrupaciones deben conducir a tablas de encaminamiento más pequeñas y a consultas más rápidas. El permitir múltiples direcciones por interfaz posibilita a un abonado que utiliza varios proveedores de acceso a través de la misma interfaz, tener direcciones distintas agrupadas bajo el espacio de direcciones de cada proveedor.

IPv6 permite tres tipos de direcciones:

- **Unidifusión (*unicast*):** un identificador para una interfaz individual. Un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.
- **Monodifusión (*anycast*):** un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección monodifusión se entrega a una de las interfaces identificadas por esa dirección (la más cercana, de acuerdo a la medida de distancia de los protocolos de encaminamiento).
- **Multidifusión (*multicast*):** un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección multidifusión se entrega a todas las interfaces identificadas por esa dirección.

CABECERA DE OPCIONES SALTO A SALTO

La cabecera de opciones salto a salto transporta información opcional que, si está presente, debe ser examinada por cada dispositivo de encaminamiento a lo largo de la ruta. Esta cabecera contiene los siguientes campos (*véase* Figura 18.12a):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Longitud de la cabecera de extensión (8 bits):** longitud de la cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
- **Opciones:** campo de longitud variable que consta de una o más definiciones de opción. Cada definición se expresa mediante tres subcampos: tipo de opción (8 bits), que identifica la opción; longitud (8 bits), que especifica la longitud en octetos del campo de datos de la opción; y datos de opción, que es una especificación de la opción de longitud variable.

En realidad, se utilizan los cinco bits menos significativos del campo tipo de opción para especificar una opción particular. Los bits más significativos indican la acción que tiene que realizar un nodo que no reconoce el tipo de opción, de acuerdo a:

- 00—ignorar esta opción y continuar procesando la cabecera.
- 01—descartar el paquete.
- 10—descartar el paquete y enviar un mensaje ICMP de problema de parámetro a la dirección origen del paquete, indicando el tipo de opción no reconocida.

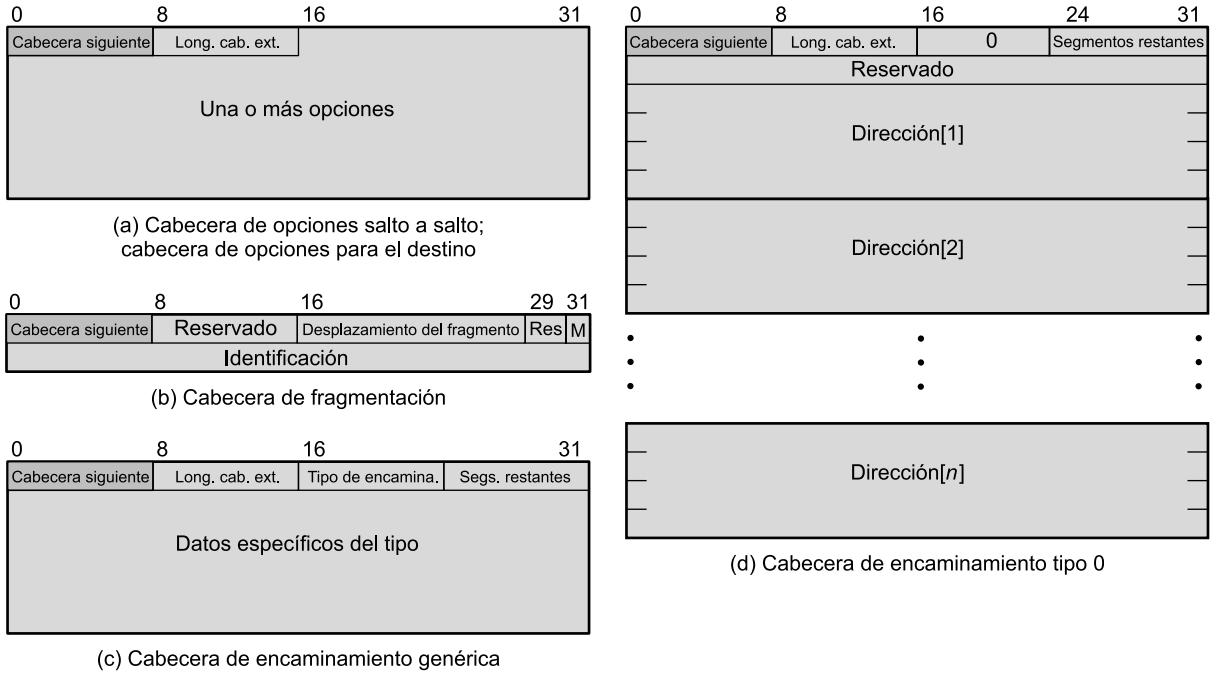


Figura 18.12. Cabecera de extensión IPv6.

- 11—descartar el paquete y, solamente si la dirección destino del paquete no es una dirección multidifusión, enviar un mensaje ICMP de problema de parámetro a la dirección origen del paquete, indicando el tipo de opción no reconocida.

El tercer bit indica si el campo de datos de la opción no cambia (0) o si puede cambiar (1) en el camino desde el origen al destino. Los datos que pueden cambiar se deben excluir de los cálculos de autentificación, como se discutirá en el Capítulo 21.

Estas convenciones para el campo del tipo de opción también se aplican a la cabecera de opciones en el destino.

Hasta ahora se han especificado cuatro opciones salto a salto:

- **Relleno1:** utilizada para insertar un byte de relleno dentro de la zona de opciones de la cabecera.
- **RellenoN:** utilizada para insertar N bytes ($N \geqslant 2$) de relleno dentro de la zona de opciones de la cabecera. Las dos opciones de relleno aseguran que la cabecera tiene una longitud múltiplo de 8 bytes.
- **Carga útil Jumbo:** se utiliza para enviar paquetes con una carga útil mayor de 65.535 octetos. El campo de datos de esta opción tiene una longitud de 32 bits y da la longitud del paquete en octetos, excluyendo la cabecera IPv6. Para estos paquetes, el campo de longitud de la carga en la cabecera IPv6 debe estar a cero y no puede haber cabecera de fragmentación. Con esta opción, IPv6 permite tamaños de paquete de hasta 4.000 millones de octetos. Esto facilita la transmisión de paquetes de vídeo grandes y posibilita que IPv6 haga el mejor uso de la capacidad disponible sobre cualquier medio de transmisión.

- **Alerta al dispositivo de encaminamiento:** informa al dispositivo de encaminamiento que el contenido de este paquete es de interés para el dispositivo de encaminamiento y para tratar adecuadamente cualquier información de control. La ausencia de esta opción en un datagrama IPv6 informa al dispositivo de encaminamiento que el paquete no contiene información necesaria para el dispositivo de encaminamiento y, por tanto, puede encaminarlo de forma segura sin ningún análisis adicional. A los computadores que originan paquetes IPv6 se les obliga a que incluyan esta opción en ciertas circunstancias. El motivo de esta opción es proporcionar un apoyo suficiente a protocolos como RSVP (*véase* Capítulo 19) que generan paquetes que necesitan ser examinados por dispositivos de encaminamiento intermedios por motivos de control de tráfico. En lugar de requerir a los dispositivos de encaminamiento intermedios que analicen en detalle la cabecera de extensión, esta opción alerta al dispositivo de encaminamiento cuando se requiere esta atención.

CABECERA DE FRAGMENTACIÓN

En IPv6, la fragmentación sólo puede ser realizada por el nodo origen, no por los dispositivos de encaminamiento a lo largo del camino del paquete. Para obtener todas las ventajas del entorno de interconexión, un nodo debe ejecutar un algoritmo de obtención de la ruta, lo que permite conocer la unidad máxima de transferencia (MTU, *Maximum Transfer Unit*) permitida por cada red en la ruta. Con este conocimiento, el nodo origen fragmentará el paquete, según se requiera, para cada dirección de destino dada. Si no se ejecuta este algoritmo, el origen debe limitar todos los paquetes a 1.280 octetos, que debe ser la mínima MTU que permitan las redes.

La cabecera de fragmentación contiene los siguientes campos (*véase* Figura 18.12b):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Reservado (8 bits):** reservado para usos futuros.
- **Desplazamiento del fragmento (13 bits):** indica dónde se sitúa en el paquete original la carga útil de este fragmento. Se mide en unidades de 64 bits. Esto implica que los fragmentos (excepto el último) deben contener un campo de datos con una longitud de múltiplo de 64 bits.
- **Reservado (2 bits):** reservado para usos futuros.
- **Indicador M (1 bit):** 1 = más fragmentos; 0 = último fragmento.
- **Identificación (32 bits):** utilizado para identificar de forma única el paquete original. El identificador debe ser único para la dirección origen y dirección destino durante el tiempo que el paquete permanece en Internet. Todos los fragmentos con el mismo identificador, dirección origen y dirección destino son reensamblados para recuperar el paquete original.

El algoritmo de fragmentación es el mismo que el descrito en la Sección 18.3.

CABECERA DE ENCAMINAMIENTO

La cabecera de encaminamiento contiene una lista de uno o más nodos intermedios por los que se pasa en el camino del paquete a su destino. Todas las cabeceras de encaminamiento comienzan con un bloque de 32 bits consistente en 4 campos de 8 bits, seguido por datos de encaminamiento específicos al tipo de encaminamiento dado (*véase* Figura 18.12c). Los cuatro campos de 8 bits son los siguientes:

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Longitud de la cabecea de extensión (8 bits):** longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
- **Tipo de encaminamiento (8 bits):** identifica una variante particular de cabecera de encaminamiento. Si un dispositivo de encaminamiento no reconoce el valor del tipo de encaminamiento, debe descartar el paquete.
- **Segmentos restantes (8 bits):** número de segmentos en la ruta que quedan; esto es, el número de nodos intermedios explícitamente contenidos en la lista que se visitarán todavía antes de alcanzar el destino.

El único formato de cabecera de encaminamiento definido en el RFC 2460 es el de la cabecera de encaminamiento tipo 0 (*véase* Figura 18.12d). Cuando se utiliza una cabecera de encaminamiento tipo 0, el nodo origen no sitúa la dirección del último destino en la cabecera IPv6. En lugar de eso, esa dirección es la última de la lista en la cabecera de encaminamiento (Dirección[*n*], en la Figura 18.12d), y la cabecera IPv6 contiene la dirección destino del primer dispositivo de encaminamiento deseado en el camino. La cabecera de encaminamiento no se examina hasta que el paquete llega al nodo identificado por la cabecera IPv6. En ese punto, el paquete IPv6 y el contenido de la cabecera se actualizan y el paquete se reenvía. La actualización consiste en situar la siguiente dirección a visitar en la cabecera IPv6 y decrementar el campo segmentos restantes en la cabecera de encaminamiento.

CABECERA DE OPCIONES PARA EL DESTINO

La cabecera de opciones para el destino lleva información opcional que, si está presente, se examina por el nodo destino del paquete. El formato de esta cabecera es el mismo que la cabecera de opciones salto a salto (*véase* Figura 18.12a).

18.6. LECTURAS Y SITIOS WEB RECOMENDADOS

[RODR02] proporciona un tratamiento completo y claro de todos los temas tratados en este capítulo. En [COME01] y [STEV94] se puede encontrar un buen estudio sobre interconexión entre redes y sobre IPv4. [HUIT98] es una descripción técnica de varios RFC que integran juntos la especificación de IPv6; el libro proporciona una discusión sobre el propósito de varias características y el funcionamiento del protocolo. En [KESH98] se proporciona un instructivo repaso a la funcionalidad presente y futura de los dispositivos de encaminamiento.

COME01 Comer, D. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture.* Upper Saddle River, NJ: Prentice Hall, 2001.

HUIT98 Huitema, C. *IPv6: The New Internet Protocol.* Upper Saddle River, NJ: Prentice Hall, 1998.

KESH98 Keshav, S., y Sharma, R. «Issues and Trends in Router Design.» *IEEE Communications Magazine*, mayo 1998.

RODR02 Rodriguez, A., *et al*., *TCP/IP Tutorial and Technical Overview*. Upper Saddle River: NJ: Prentice Hall, 2002.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols.* Reading, MA: Addison-Wesley, 1994.

SITIOS WEB RECOMENDADOS

- **IPv6:** información sobre IPv6 y temas relacionados.
- **Página de información sobre IPv6:** incluye material introductorio, noticias sobre desarrollos recientes de productos IPv6 y enlaces relacionados.
- **Foro IPv6:** se trata de un consorcio de fabricantes que promociona productos relacionados con IPv6. Incluye una serie de documentos introductorios y artículos.

18.7. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

clase de tráfico
difusión
dispositivo de encaminamiento
fragmentación
interconexión de redes
internet
intranet
IPv4
IPv6
máscara de subred
monodifusión
multidifusión
protocolo de mensajes de control de internet (ICMP)
protocolo Internet (IP)
reensamblado
segmentación
sistema final
sistema intermedio
subred
tiempo de vida del datagrama

CUESTIONES DE REPASO

18.1. Dé algunas razones para usar fragmentación y reensamblado.

18.2. Enumere los requisitos de un mecanismo de interconexión de redes.

18.3. ¿Cuáles son los pros y los contras de limitar el reensamblado a los sistemas finales en lugar de permitirlo en los dispositivos de encaminamiento?

18.4. Explique la función de los tres indicadores en la cabecera de IPv4.

18.5. ¿Cómo se calcula la suma de comprobación de la cabecera de IPv4?

18.6. ¿Qué diferencia existe entre los campos clase de tráfico y etiqueta de flujo en la cabecera de IPv6?

18.7. Explique brevemente los tres tipos de direcciones IPv6.

18.8. ¿Cuál es el propósito de cada uno de los tipos de cabeceras presentes en IPv6?

EJERCICIOS

18.1. En la discusión sobre IP, se mencionó que el *identificador*, el *indicador de no fragmentar* y el *tiempo de vida* se hallan presentes en la primitiva *Send* pero no en la primitiva

Deliver, ya que esos parámetros no son competencia de IP. Indique, para cada una de estas primitivas, si es competencia de la entidad IP en el origen, de la entidad IP en cada dispositivo de encaminamiento intermedio o de la entidad IP en el sistema final destino. Justifique su respuesta.

18.2. ¿Cuál es la información suplementaria de la cabecera en el protocolo IP?

18.3. Describa algunas circunstancias en las que sería deseable utilizar encaminamiento en el origen en lugar de dejar a los dispositivos de encaminamiento que realicen la decisión de encaminamiento.

18.4. A causa de la fragmentación, un datagrama IP puede llegar en varios trozos, no necesariamente en el orden adecuado. La entidad IP en el sistema final receptor debe acumular estos fragmentos hasta que se reconstruya el datagrama original.

a) Considere que la entidad IP crea una memoria temporal para reensamblar el campo de datos del datagrama original. Conforme se va realizando el reensamblado, la memoria temporal contendrá bloques de datos y zonas vacías («agujeros») entre los bloques de datos. Describa un algoritmo para reensamblar datagramas basado en este concepto.

b) Para el algoritmo de la parte (a) es necesario hacer un seguimiento a los agujeros. Describa un mecanismo sencillo para hacer esto.

18.5. Un datagrama de 4.480 octetos se va a transmitir y se necesita fragmentar ya que va a pasar por una red Ethernet con un campo máximo de carga útil de 1.500 octetos. Muestre los valores de los campos longitud total, indicador de más segmentos y desplazamiento de fragmento en cada uno de los fragmentos resultantes.

18.6. Se necesita que la suma de comprobación de IP se recalcule en los dispositivos de encaminamiento a causa de los cambios en la cabecera IP, como el que ocurre en el campo tiempo de vida. Es posible recalcular esta suma desde cero. Sugiera un procedimiento que suponga menos cálculos. *Sugerencia:* suponga que el valor en el octeto k es cambiado por Z = valor_nuevo – valor_viejo; considere el efecto de este cambio en la suma de comprobación.

18.7. Se va a segmentar un datagrama. ¿Qué opciones del campo de opción se necesitan copiar en la cabecera de cada fragmento y cuáles se necesitan copiar sólo en el primer fragmento? Justifique el tratamiento de cada opción.

18.8. Un mensaje de la capa de transporte, que contiene 1.500 bits de datos y 160 bits de cabecera, se envía a la capa internet, la cual incorpora otros 160 bits de cabecera. El resultado se transmite a través de dos redes que utilizan cada una 24 bits de cabecera de paquete. La red destino tiene un tamaño de paquete máximo de 800 bits. ¿Cuántos bits, incluyendo cabeceras, se entregan al protocolo de la capa de red en el destino?

18.9. Se va a utilizar la arquitectura sugerida por la Figura 18.2. ¿Qué funciones se deberían añadir a los dispositivos de encaminamiento para aliviar algunos de los problemas causados por la desigualdad entre redes locales y de transporte a larga distancia?

18.10. ¿Debería existir una relación entre la interconexión entre redes y el encaminamiento interno de red? ¿Por qué sí o por qué no?

18.11. Compare los campos individuales de la cabecera IPv4 con los de la cabecera IPv6. Compare las posibilidades proporcionadas por cada uno de los campos de IPv4 con los de IPv6.

18.12. Justifique el orden recomendado de las cabeceras de extensión de IPv6 (por ejemplo, ¿por qué va primero la cabecera de opciones salto-a-salto?, ¿por qué la cabecera de encaminamiento está antes que la cabecera de fragmentación?, y así hasta la cabecera final).

18.13. El estándar IPv6 afirma que si un paquete con una etiqueta de flujo distinta de cero llega a un dispositivo de encaminamiento y éste no tiene información para esa etiqueta de flujo, el dispositivo de encaminamiento debería ignorar la etiqueta de flujo y reenviar el paquete.

a) ¿Cuáles son las desventajas de tratar este evento como un error, descartar el paquete y enviar un mensaje ICMP?

b) ¿Existen situaciones en las que encaminar el paquete como si su etiqueta de flujo fuera cero causará un resultado erróneo? Explíquelo.

18.14. El mecanismo de flujo de IPv6 supone que el estado asociado con una etiqueta de flujo dada se almacena en los dispositivos de encaminamiento. Por tanto, éstos saben cómo tratar los paquetes que llevan esa etiqueta de flujo. Un requisito de diseño es eliminar en los dispositivos de encaminamiento las etiquetas de flujo que no se van a utilizar más (etiquetas de flujo obsoletas).

a) Suponga que una fuente siempre envía un mensaje de control a todos los dispositivos de encaminamiento afectados suprimiendo una etiqueta de flujo cuando el origen acabe con ese flujo. En este caso, ¿cómo podría persistir una etiqueta de flujo antigua?

b) Sugiera mecanismos del origen y de los dispositivos de encaminamiento para superar el problema de las etiquetas de flujo antiguas.

18.15. Una cuestión que se plantea es qué paquetes generados por un origen deberían llevar etiquetas de flujo IPv6 distintas de cero. Para algunas aplicaciones, la respuesta es obvia. Los intercambios pequeños de datos deberían tener una etiqueta de flujo cero, ya que no merece la pena crear un flujo para unos pocos paquetes. Los flujos en tiempo real deberían tener una etiqueta de flujo; estos flujos fueron la causa primera de que se crearan etiquetas de flujo. Una cuestión más difícil es qué hacer con entidades paritarias que están enviando una gran cantidad de tráfico con el mejor esfuerzo (por ejemplo, las conexiones TCP). Describa un caso para asignar una única etiqueta de flujo a cada conexión TCP de gran duración. Describa un caso para no hacer esto.

18.16. Las especificaciones originales de IPv6 combinaban los campos de etiqueta de flujo y prioridad en un solo campo de etiqueta de flujo de 28 bits. Esto permitía a los flujos redefinir la interpretación de los diferentes valores de prioridad. Sugiera una razón por la que la especificación final incluye un campo de prioridad en un campo distinto.

18.17. Para el encaminamiento IPv6 tipo 0, especifique el algoritmo para actualizar las cabeceras IPv6 y de encaminamiento en los nodos intermedios.

CAPÍTULO 19

Funcionamiento de la interconexión de redes

19.1. Multidifusión
Requisitos para la multidifusión
Protocolo de gestión de grupos de Internet

19.2. Protocolos de encaminamiento
Sistemas autónomos
Estrategias de encaminamiento
Protocolo de pasarela frontera
Protocolo del primer camino más corto disponible

19.3. Arquitectura de servicios integrados
Tráfico en Internet
Enfoque ISA
Componentes ISA
Servicios ISA
Disciplinas de atención de cola
Protocolo de reserva de recursos

19.4. Servicios diferenciados
Servicios
Octeto DS
Configuración y funcionamiento de los DS
Comportamiento por salto

19.5. Lecturas y sitios web recomendados

19.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- El envío de un paquete desde un origen a múltiples destinos se denomina multidifusión. La multidifusión plantea nuevas cuestiones de diseño en las áreas de direccionamiento y encaminamiento.
- Los protocolos de encaminamiento en una interconexión de redes funcionan de modo similar a los que se utilizan en redes de conmutación de paquetes. Un protocolo de encaminamiento se utiliza en una interconexión de redes para intercambiar información sobre accesibilidad y retardos de tráfico, permitiendo a cada encaminador construir la tabla de encaminamiento del siguiente salto para las rutas que atraviesan el conjunto de redes interconectadas. Normalmente, se utilizan protocolos de encaminamiento relativamente simples entre sistemas autónomos pertenecientes a una interconexión de redes mayor y protocolos de encaminamiento más complejos dentro de cada uno de los sistemas autónomos.
- La arquitectura de servicios integrados surge como respuesta a la creciente variedad y volumen de tráfico que se experimenta en redes privadas e Internet. Proporciona un marco para el desarrollo de protocolos como RSVP para tratar tráfico multimedia/multidifusión y orienta a los fabricantes de dispositivos de encaminamiento en el desarrollo de técnicas eficientes para ocuparse de una variada carga.
- La arquitectura de servicios diferenciados se diseña para proporcionar una herramienta simple, fácil de implementar y que genere una escasa sobrecarga, para permitir ofrecer un conjunto de servicios de red que se distingan en función del rendimiento resultante. Los servicios diferenciados se proporcionan basándose en una etiqueta de 6 bits de la cabecera IP que clasifica el tráfico según el tipo de servicio que han de darle a ese tráfico los dispositivos de encaminamiento.

A medida que Internet y las redes privadas crecen en tamaño, entra firmemente en escena un nuevo tipo de estaciones con nuevas demandas. Las aplicaciones cliente/servidor de gran volumen superan a las conversaciones de bajo volumen de tráfico TELNET. A esto se le ha añadido recientemente el tremendo volumen de tráfico web, compuesto cada vez más por gráficos. Actualmente, las aplicaciones de voz y vídeo en tiempo real se han sumado a esta carga.

Para hacer frente a estas demandas no es suficiente aumentar la capacidad de Internet. Se necesitan métodos efectivos y sensibles de gestión de tráfico y de control de congestión. Históricamente, las redes basadas en IP han sido capaces de proporcionar un servicio simple de entrega de mejor esfuerzo a todas las aplicaciones que utilizan una interconexión de redes. Pero las necesidades de los usuarios han cambiado. Una compañía puede haber gastado millones de dólares instalando una red basada en IP diseñada para transportar datos entre LAN y, sin embargo, ahora descubre que las nuevas aplicaciones en tiempo real, multimedia y de multidifusión no funcionan bien en esta configuración. El único esquema de interconexión de redes diseñado para dar soporte desde el primer día al tráfico tradicional TCP y UDP en tiempo real es ATM. Sin embargo, la fiabilidad en ATM implica o bien construir una segunda infraestructura de interconexión redes para el tráfico en tiempo real, o reemplazar la configuración existente basada en IP por ATM, siendo ambas alternativas costosas.

Por tanto, existe una imperiosa necesidad de ser capaz de dar soporte a una gran diversidad de tráfico con gran variedad de requisitos en cuanto a calidad de servicio (QoS, *Quality of Service*), dentro de la arquitectura TCP/IP. Este capítulo examina las funciones y servicios de interconexión de redes diseñados para satisfacer esta necesidad.

El capítulo empieza con un estudio sobre la multidifusión. Después, exploramos la cuestión de los algoritmos de encaminamiento para la interconexión de redes. A continuación, se examina la arquitectura de servicios integrados (ISA, *Integrated Services Architecture*), que proporcionan un entorno de trabajo para los servicios de redes interconectadas actuales y futuros. Finalmente, examinaremos el concepto de servicios diferenciados.

La Figura 2.15 destaca la posición de los protocolos estudiados en este capítulo dentro de la arquitectura de protocolos TCP/IP.

19.1. MULTIDIFUSIÓN

Normalmente, una dirección IP hace referencia a un computador individual en una red en particular. Pero IP también tiene cabida para direcciones que hagan referencia a un grupo de computadores en una o más redes. Tales direcciones se conocen como **direcciones de multidifusión** y el hecho de enviar un paquete desde un origen a los miembros de un grupo de multidifusión se conoce como **multidifusión**.

La multidifusión tiene una serie de aplicaciones prácticas. Por ejemplo:

- **Multimedia:** un grupo de usuarios «sintoniza» una transmisión de vídeo o audio proveniente de una estación multimedia origen.
- **Teleconferencia:** un grupo de estaciones de trabajo forman un grupo de multidifusión de forma que la transmisión desde cualquier miembro del grupo es recibida por el resto del grupo.
- **Bases de datos:** todas las copias de un fichero o base de datos replicados se actualizan al mismo tiempo.
- **Computación distribuida:** los resultados intermedios se envían a todos los participantes.
- **Trabajo en grupo en tiempo real:** los ficheros, gráficos y mensajes se intercambian en tiempo real entre todos los miembros activos.

La multidifusión realizada dentro del ámbito de un único segmento LAN es directa. El protocolo IEEE 802 y otros protocolos LAN incluyen direcciones que permiten la multidifusión a nivel MAC. Un paquete con una dirección de multidifusión se transmite en un segmento LAN. Aquellas estaciones que sean miembros del grupo de multidifusión correspondiente reconocen la dirección de multidifusión y aceptan el paquete. En este caso, sólo se transmite una copia del paquete. Esta técnica funciona debido a la naturaleza de difusión de una LAN: una transmisión desde cualquier estación se recibe por todas las estaciones de la LAN.

En un entorno de redes interconectadas, la multidifusión es mucho más difícil de acometer. Para ver esto, considere la configuración de la Figura 19.1; se tienen varias LAN interconectadas mediante dispositivos de encaminamiento. Los dispositivos de encaminamiento están conectados entre sí mediante enlaces de alta velocidad o a través de una red de área amplia (red N4). A cada enlace y red se le asocia un coste en cada dirección, indicado por el valor mostrado en la dirección del encaminador hacia el enlace o la red. Suponga que un servidor de multidifusión en la red N1 está transmitiendo paquetes a una dirección de multidifusión que representa las estaciones de trabajo indicadas en las redes N3, N5 y N6. Suponga que el servidor no conoce la localización de los miembros del grupo de multidifusión. Entonces, una manera de asegurar que el paquete lo reciben todos los miembros del grupo consiste en **difundir** una copia de cada paquete en cada red de la configuración sobre la ruta de menor coste para cada red. Por ejemplo, un paquete se dirigiría a N3 y atravesaría N1, el enlace L3 y N3. El encaminador B es responsable de traducir la dirección de

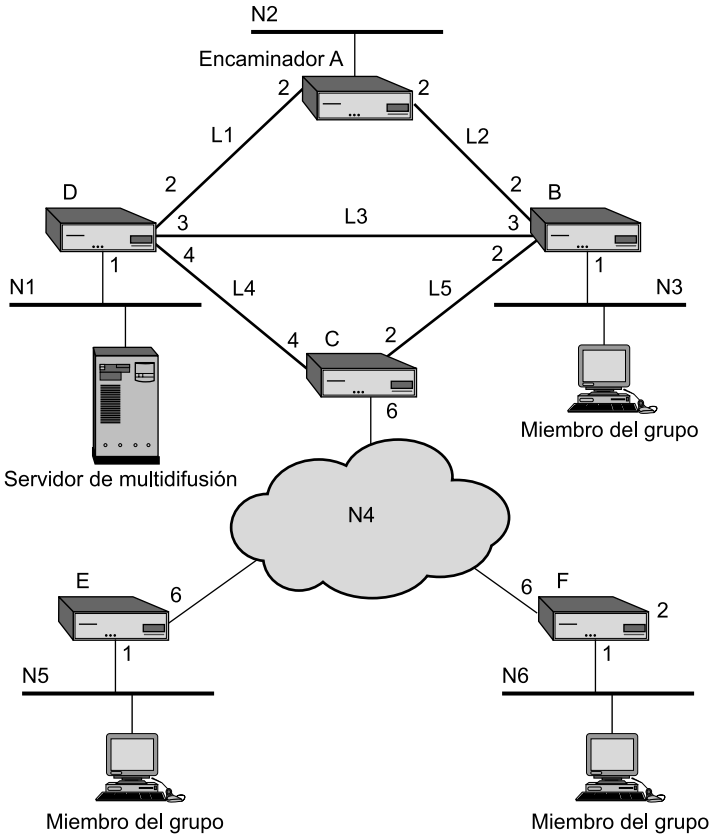


Figura 19.1. Configuración de ejemplo.

multidifusión de nivel IP a una dirección de multidifusión de nivel MAC antes de transmitir la trama MAC en N3. La Tabla 19.1 resume el número de paquetes generados en los diferentes enlaces y redes para transmitir un paquete a un grupo de multidifusión mediante este método. En esta tabla, el origen es el servidor de multidifusión de la red N1 de la Figura 19.1; la dirección de multidifusión incluye los miembros del grupo que se encuentran en N3, N5 y N6. Cada columna de la tabla se refiere a la ruta tomada desde la estación origen hasta un dispositivo de encaminamiento destino conectado a una red destino determinado. Cada fila de la tabla corresponde a una red o enlace de la configuración de la Figura 19.1. Cada entrada de la tabla muestra el número de paquetes que atraviesan una red o enlace dado para una ruta concreta. En este caso, se necesitan un total de 13 copias del paquete.

Suponga ahora que el sistema origen conoce la localización de cada miembro del grupo de multidifusión. Es decir, la fuente tiene una tabla que traduce la dirección de multidifusión en una lista de redes que contienen a los miembros del grupo. En este caso, la fuente necesita solamente enviar los paquetes a aquellas redes que contengan miembros del grupo. Podríamos denominar esta técnica como la estrategia de **unidifusión múltiple**. La Tabla 19.1 muestra que en este caso se necesitan 11 paquetes.

Ambas estrategias, difusión y unidifusión múltiple, son ineficientes, ya que generan copias innecesarias del paquete original. En una estrategia de **multidifusión** genuina se emplea el siguiente método:

Tabla 19.1. Tráfico generado por varias estrategias de multidifusión

	(a) Difusión					(b) Unidifusión múltiple				(c) Multidifusión
	S → N2	S → N3	S → N5	S → N6	Total	S → N3	S → N5	S → N6	Total	
N1	1	1	1	1	4	1	1	1	3	1
N2										
N3		1			1	1			1	1
N4			1	1	2		1	1	2	2
N5			1		1		1		1	1
N6				1	1			1	1	1
L1	1				1					
L2										
L3		1			1	1			1	1
L4			1	1	2		1	1	2	1
L5										
Total	2	3	4	4	13	3	4	4	11	8

1. Se determina el camino de menor coste desde el origen a cada red que incluya miembros del grupo de multidifusión. Se obtiene así un árbol de expansión[1] de la configuración. Observe que no es un árbol de expansión completo de la configuración. En cambio, se trata de un árbol de expansión que incluye sólo aquellas redes que contienen miembros del grupo.
2. La fuente transmite un único paquete a través del árbol de expansión.
3. Los dispositivos de encaminamiento replican el paquete sólo en los puntos de bifurcación del árbol de expansión.

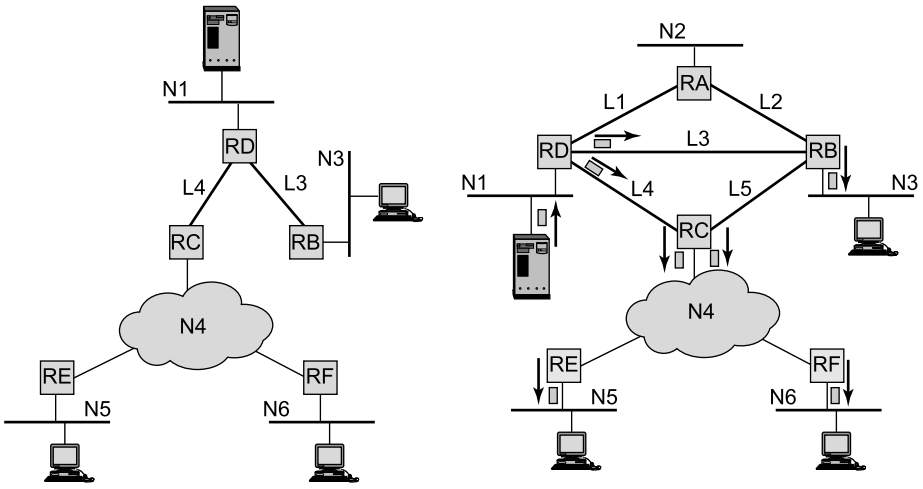
La Figura 19.2a muestra el árbol de expansión para la transmisión desde el origen al grupo de multidifusión, y la Figura 19.2b muestra este método en acción.

El origen transmite un único paquete sobre N1 al dispositivo de encaminamiento D. D hace dos copias del paquete, para transmitirlos por los enlaces L3 y L4. B recibe el paquete por L3 y lo transmite en N3, donde es recibido por los miembros del grupo de multidifusión de esa red. Mientras tanto, C recibe el paquete enviado por L4. Ahora debe entregar el paquete a E y F. Si N4 fuera una red de difusión (por ejemplo, una LAN IEEE 802), C sólo necesitaría transmitir una copia del paquete para que ambos dispositivos de encaminamiento lo recibieran. Si N4 es una red WAN de conmutación de paquetes, entonces C debe hacer dos copias del paquete y dirigir una a E y otra a F. Cada uno de estos dispositivos de encaminamiento, a su vez, retransmite el paquete recibido en N5 y N6, respectivamente. Como muestra la Tabla 19.1, la técnica de multidifusión sólo requiere ocho copias del paquete.

REQUISITOS PARA LA MULTIDIFUSIÓN

En una transmisión en unidifusión usual a través de una interconexión de redes, en la que cada datagrama tiene una única red destino, la tarea de cada dispositivo de encaminamiento consiste en reenviar el datagrama por el camino más corto desde ese encaminador hasta la red destino. En una

[1] El concepto de árbol de expansión fue presentado en nuestra exposición sobre puentes en el Capítulo 15. Un árbol de expansión de un grafo consta de todos los nodos del grafo más un subconjunto de los enlaces (arcos) del grafo que proporcione conectividad (exista un camino entre cualesquiera dos nodos) sin bucles cerrados (es decir, que exista sólo un camino entre cualesquiera dos nodos).



(a) Árbol de expansión desde la fuente al grupo de multidifusión

(b) Paquetes generados por la transmisión en multidifusión

Figura 19.2. Ejemplo de transmisión en multidifusión.

transmisión en multidifusión, el dispositivo de encaminamiento puede necesitar reenviar dos o más copias de un datagrama recibido. En nuestro ejemplo, los encaminadores D y C deben reenviar dos copias de un único datagrama recibido.

De este modo, podríamos esperar que la funcionalidad global del encaminamiento de multidifusión sea más compleja que el encaminamiento con un solo destino. A continuación, se enumeran las funciones que se requieren:

1. Se necesita una convención para identificar las direcciones de multidifusión. En IPv4 se reserva para este propósito la clase D de direcciones. Éstas son direcciones de 32 bits con los 4 bits más significativos fijados a 1110, seguidos por un identificador de grupo de 28 bits. En IPv6, una dirección de multidifusión de 128 bits está formada por un prefijo de 8 bits con valor 1, un campo de indicadores de 4 bits, un campo de ámbito de 4 bits y un identificador de grupo de 112 bits. Actualmente, el campo de indicadores sólo indica si la dirección está permanentemente asignada o no. El campo de ámbito indica el ámbito de aplicabilidad de la dirección, un rango que va desde una única red a la red global.
2. Cada nodo (encaminador o fuente que participe en el algoritmo de encaminamiento) debe traducir una dirección IP de multidifusión a una lista de redes que contengan miembros de este grupo. Esta información le permite al nodo construir un árbol de expansión de camino mínimo hacia todas las redes que contengan miembros del grupo.
3. Un dispositivo de encaminamiento debe traducir una dirección de multidifusión IP a una dirección de multidifusión de red con objeto de entregar en la red destino un datagrama IP de multidifusión. Por ejemplo, en redes IEEE 802, una dirección a nivel MAC es de 48 bits. Si el bit más significativo es 1, entonces se trata de una dirección de multidifusión. Por tanto, para la entrega en multidifusión, un encaminador conectado a una red IEEE 802 debe traducir una dirección de multidifusión de 32 bits en IPv4, o de 128 bits en IPv6, a una dirección de multidifusión del nivel MAC de IEEE 802 de 48 bits.
4. Aunque algunas direcciones de multidifusión pueden asignarse permanentemente, el caso más usual es que las direcciones de multidifusión sean generadas dinámicamente y que las

estaciones individuales puedan unirse o abandonar los grupos de multidifusión dinámicamente. De esta manera, se necesita un mecanismo por el que un computador individual informe al encaminador conectado a su misma red de su inclusión o exclusión en un grupo de multidifusión.

5. Los dispositivos de encaminamiento deben intercambiar dos tipos de información. En primer lugar, los encaminadores necesitan saber qué redes contienen miembros de un grupo de multidifusión determinado. En segundo lugar, los dispositivos de encaminamiento necesitan obtener suficiente información para calcular los caminos más cortos a cada red que contenga miembros del grupo. Estos requisitos implican la necesidad de un protocolo de encaminamiento para multidifusión. El análisis de tales protocolos está fuera del alcance de este libro.
6. Se necesita un algoritmo de encaminamiento para calcular los caminos más cortos a todos los miembros del grupo.
7. Cada dispositivo de encaminamiento debe determinar la ruta de encaminamiento en multidifusión basándose en las direcciones fuente y destino.

Este último punto es una sutil consecuencia del uso de direcciones de multidifusión. Para ilustrar esta cuestión, considere de nuevo la Figura 19.1. Si el servidor de multidifusión transmite un paquete en unidifusión dirigido a un computador en la red N5, el encaminador D reenvía el paquete a C, quien a su vez lo reenvía a E. De forma similar, D reenviaría a B los paquetes dirigidos a un computador de la red N3. Pero ahora suponga que el servidor transmite el paquete con una dirección de multidifusión que incluya computadores de N3, N5 y N6. Como se ha comentado anteriormente, D hace dos copias del paquete y envía una a B y otra a C. Ahora, ¿qué hará C cuando reciba un paquete con esa dirección de multidifusión? C sabe que este paquete va dirigido a las redes N3, N5 y N6. Un esquema simple consistiría en que C calculara el camino más corto a cada una de estas tres redes. De esta forma se construye el árbol de expansión de camino mínimo mostrado en la Figura 19.3. Como resultado, C envía dos copias del paquete por la red N4, una dirigida a la red N5 y la otra a la red N6. Pero además envía una copia del paquete a B para su entrega en N3. De esta manera B recibirá dos copias del paquete, una de D y otra de C. Claramente, esto no es lo que pretendía el computador de la red N1 cuando emitió el paquete.

Para evitar la duplicación innecesaria de paquetes, cada encaminador debe encaminar los paquetes basándose en la fuente y el destino de la multidifusión. Cuando C recibe un paquete dirigido al grupo de multidifusión desde una fuente en N1, C debe calcular el árbol de expansión con N1 como raíz (como se muestra en la Figura 19.2a) y encaminar según este árbol de expansión.

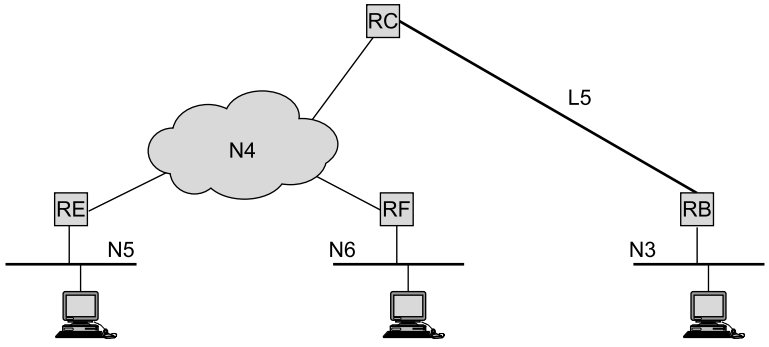


Figura 19.3. Árbol de expansión del encaminador C al grupo de multidifusión.

PROTOCOLO DE GESTIÓN DE GRUPOS DE INTERNET

Las estaciones y encaminadores utilizan el protocolo de gestión de grupos de Internet (IGMP, *Internet Group Management Protocol*), definido en el RFC 3376, para intercambiar información sobre la pertenencia a los grupos de multidifusión en una LAN. IGMP aprovecha la naturaleza de difusión de las LAN para proporcionar una técnica eficiente para el intercambio de información entre múltiples estaciones y encaminadores. En general, IGMP ofrece dos funciones principales:

1. El envío de mensajes desde las estaciones a los encaminadores para subscribirse y para abandonar grupos de multidifusión definidos por una dirección de multidifusión dada.
2. La comprobación periódica de los encaminadores sobre qué grupos de multidifusión interesan a qué estaciones.

La última versión de IGMP es la 3. En IGMPv1, las estaciones podían unirse a un grupo de multidifusión y los encaminadores utilizaban un temporizador para eliminar miembros de los grupos. IGMPv2 permitió a las estaciones abandonar expresamente un grupo. Las dos primeras versiones utilizaban básicamente el modelo de operación siguiente:

- Los receptores deben subscribirse a los grupos de multidifusión.
- Las fuentes no tienen que subscribirse a los grupos de multidifusión.
- Cualquier estación puede enviar tráfico a cualquier grupo de multidifusión.

Este paradigma es muy general, pero tiene varias debilidades:

1. El envío de información no deseada a los grupos de multidifusión es fácil. Incluso si existen filtros a nivel de aplicación para descartar paquetes no deseados, esos paquetes consumen todavía recursos valiosos de la red y del receptor que tiene que procesarlos.
2. La creación de los árboles de distribución de multidifusión es problemática, principalmente porque la localización de las fuentes se desconoce.
3. Encontrar direcciones de multidifusión únicas globalmente es difícil. Siempre es posible que otro grupo de multidifusión utilice la misma dirección de multidifusión.

IGMPv3 aborda estas debilidades con las siguientes medidas:

1. Permitiendo a las estaciones especificar la lista de equipos desde las que quieren recibir tráfico. El tráfico proveniente de otras estaciones es bloqueado en los encaminadores.
2. Permitiendo a las estaciones bloquear los paquetes que provengan de fuentes que envíen tráfico no deseado[2].

En el resto de esta sección se tratará IGMPv3.

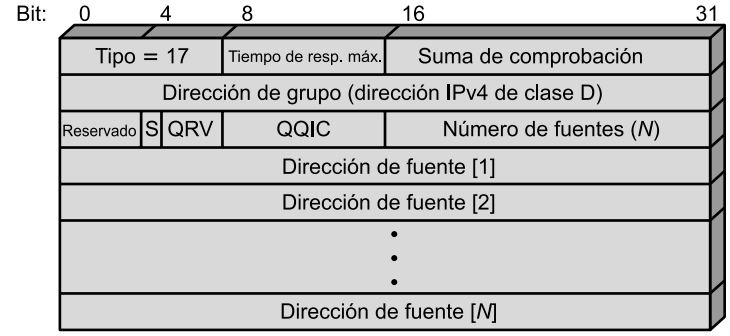
Formato del mensaje IGMP

Todos los mensajes de IGMP se transmiten en datagramas IP. La versión actual define dos tipos de mensajes: «consulta de pertenencia a grupo» e «informe de pertenencia a grupo».

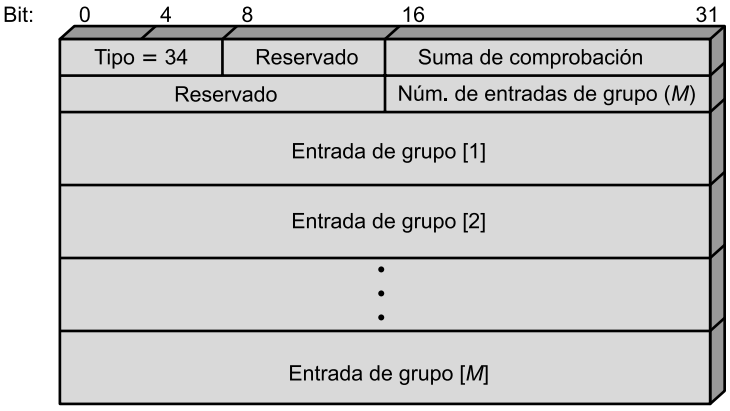
Los mensajes de **consulta de pertenencia a grupo** (*Membership Query*) los envían los encaminadores de multidifusión. Existen tres subtipos: una **consulta general**, empleada para descubrir

[2] La anterior visión general de IGMP está basada en la de Christo Gkantsidis (http://cc.gatech.edu/~gantsich/igmpv3.htm).

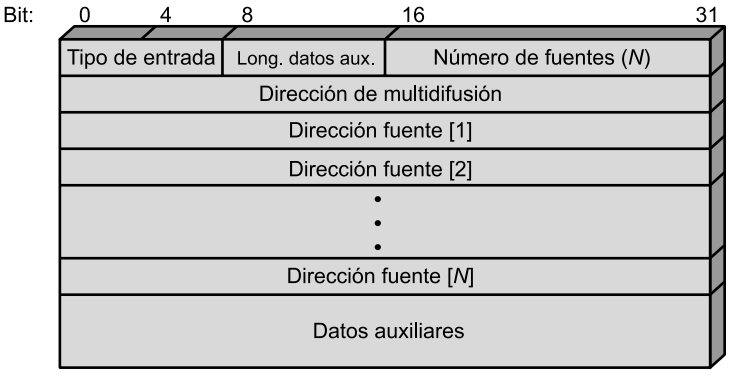
qué grupos tienen miembros en una red conectada al encaminador, una **consulta de grupo específico**, utilizada para averiguar si un grupo determinado tiene algún miembro en una red conectada al encaminador, y una **consulta de grupo y fuente específicos,** utilizado para averiguar si alguno de los dispositivos conectados desea recibir los paquetes enviados a una dirección de multidifusión especificada, desde alguna de las fuentes especificadas en una lista. La Figura 19.4a muestra el formato del mensaje, que se compone de los siguientes campos:



(a) Mensaje de consulta de pertenencia a grupo



(b) Mensaje de informe de pertenencia a grupo



(c) Entrada de grupo

Figura 19.4. Formato de los mensajes IGMPv3.

- **Tipo:** indica el tipo de este mensaje.
- **Tiempo de respuesta máximo:** especifica el tiempo máximo de respuesta tolerado antes de enviar un informe de respuesta en unidades de 1/10 segundos.
- **Suma de comprobación:** un código de detección de errores, calculado como el complemento a uno de la suma de todas las palabras de 16 bits del mensaje. A efectos de cálculo, el campo de suma de comprobación se inicializa a cero. Éste es el mismo algoritmo de suma de comprobación que el calculado en IPv4.
- **Dirección de grupo:** cero para un mensaje de consulta general. Una dirección IP de grupo de multidifusión válida cuando se envía una consulta de grupo específico, o una consulta de grupo y fuente específicos.
- **Indicador S:** cuando su valor es uno, indica a todos los encaminadores de multidifusión que lo reciban que deben suprimir las actualizaciones habituales del temporizador que realizan tras recibir una consulta.
- **Indicador de robustez del solicitante, o QRV (*Querier's Robutness Variable*):** si su valor es distinto de cero, el campo QRV contiene el valor RV utilizado por el solicitante (es decir, el emisor de la consulta). Los encaminadores adoptan como su propio valor de RV el valor del RV de la consulta más recientemente recibida, a menos que haya sido cero, en cuyo caso los receptores utilizan un valor por defecto o un valor estático de configuración. El RV impone el número de veces que una estación retransmitirá un informe para asegurar que todos los encaminadores de multidifusión conectados lo reciben.
- **Intervalo de consulta del consultante, o QQIC (*Querier's Querier Interval Code*):** especifica el valor de QI empleado por el consultante, que es un temporizador para enviar múltiples consultas. Los encaminadores que no son consultantes en ese momento adoptan como valor propio de QI el valor de QI de la consulta más recientemente recibida, a menos que fuera cero, en cuyo caso usan el valor de QI por defecto.
- **Número de fuentes:** especifica cuántas direcciones de fuentes hay en la consulta. Este valor es diferente a cero sólo para la consulta de grupo y fuente específicos.
- **Direcciones de fuentes:** si el número de fuentes es *N*, entonces hay *N* direcciones de unidifusión de 32 bits adjuntas al mensaje.

Un mensaje de **informe de pertenencia a grupo** (*Membership Report*) se compone de los siguientes campos:

- **Tipo:** indica el tipo de este mensaje.
- **Suma de comprobación:** un código de detección de errores, calculado como el complemento a uno de la suma de todas las palabras de 16 bits del mensaje.
- **Número de entradas de grupo:** especifica cuántas entradas de grupo están presentes en el informe.
- **Entradas de grupo:** si el número de entradas es *M*, entonces hay *M* direcciones de unidifusión de 32 bits adjuntas al mensaje.

Una entrada de grupo incluye los siguientes campos:

- **Tipo de entrada:** define el tipo de la entrada, como se describe posteriormente.
- **Longitud de datos auxiliares:** indica la longitud del campo de datos auxiliares, en palabras de 32 bits.

- **Número de fuentes:** especifica cuántas direcciones de fuentes hay en esta entrada.
- **Dirección de multidifusión:** la dirección IP de multidifusión a la que concierne la entrada.
- **Direcciones de las fuentes:** si el número de fuentes es *N*, entonces hay *N* direcciones de unidifusión de 32 bits adjuntas al mensaje.
- **Datos auxiliares:** información adicional concerniente a esta entrada. Actualmente, no existen valores definidos para los datos auxiliares.

Funcionamiento de IGMP

El objetivo de que un computador utilice IGMP es darse a conocer como un miembro del grupo con una dirección de multidifusión concreta a otros computadores de la LAN y a todos los dispositivos de encaminamiento de la LAN. IGMPv3 introduce en las estaciones la capacidad de señalizar su pertenencia a un grupo con la posibilidad de filtrar fuentes. Una estación puede indicar que quiere recibir tráfico de todas las fuentes que envíen a un grupo exceptuando algunas fuentes específicas (a lo que se denomina modo EXCLUSIVO), o que quiere recibir tráfico sólo de algunas fuentes concretas de las que envían al grupo (modo INCLUSIVO). Para unirse a un grupo, una estación envía un mensaje IGMP de informe de pertenencia a grupo, en el que el campo de dirección de grupo sea la dirección de multidifusión del grupo. Este mensaje se envía en un datagrama IP con la misma dirección de multidifusión destino. En otras palabras, el campo de dirección de grupo del mensaje IGMP y el campo de dirección de destino de la cabecera del datagrama IP son el mismo. Todas las estaciones que sean en ese momento miembros de este grupo de multidifusión reciben el mensaje y descubren así la existencia del nuevo miembro del grupo. Cada dispositivo de encaminamiento conectado a la LAN debe atender todas las direcciones IP de multidifusión para poder recibir todos los informes.

Para mantener una lista actualizada válida de las direcciones de grupo activas, un encaminador de multidifusión emite periódicamente mensajes de consulta general, enviados en datagramas IP con la dirección de multidifusión *todas las estaciones*. Cada estación que todavía quiera permanecer como miembro de uno o más grupos de multidifusión debe atender los datagramas con dirección todas las estaciones. Cuando una de estas estaciones recibe la solicitud, debe responder con un mensaje de informe por cada grupo al que afirma pertenecer.

Observe que el dispositivo de encaminamiento de multidifusión no necesita conocer la identidad de cada computador miembro de un grupo. En su lugar, sólo necesita saber que existe al menos un miembro del grupo todavía activo. Por tanto, cada estación perteneciente a un mismo grupo que reciba una consulta inicia un temporizador con un retardo aleatorio. Toda estación que reciba el mensaje de otro computador reclamando su pertenencia al grupo cancelará su propio informe. Si no recibe ningún informe y expira el temporizador, el computador envía su informe. Con este esquema, solamente un miembro de cada grupo debe proporcionar un informe al dispositivo de encaminamiento de multidifusión.

Cuando una estación deja un grupo, envía un mensaje de abandono de grupo a la dirección estática de multidifusión de todos los encaminadores. Esto se lleva a cabo mediante el envío de un mensaje de informe de pertenencia a grupo con la opción de EXCLUSIÓN y una lista vacía de direcciones de fuentes. En otras palabras, todas las fuentes han de ser excluidas, dejando efectivamente el grupo. Cuando un encaminador recibe este mensaje para un grupo que tenga miembros en la interfaz de recepción, éste necesita determinar si queda algún miembro en el grupo. Para ello, el encaminador utiliza el mensaje de consulta de grupo específico.

Pertenencia a grupos en IPv6

IGMP se definió para operar con IPv4 y hace uso de direcciones de 32 bits. Las redes IPv6 requieren la misma funcionalidad. En lugar de definir una versión separada de IGMP para IPv6, su funcionalidad se ha incorporado en la nueva versión del protocolo de mensajes de control de Internet (ICMPv6). ICMPv6 incluye toda la funcionalidad de ICMPv4 e IGMP. Para dar soporte a la multidifusión, ICMPv6 incluye un mensaje de consulta de pertenencia a grupo y un mensaje de informe de pertenencia a grupo, que se utilizan en la misma forma que en IGMP.

19.2. PROTOCOLOS DE ENCAMINAMIENTO

En una interconexión de redes, los dispositivos de encaminamiento son responsables de recibir y reenviar los paquetes a través del conjunto de redes interconectadas. Cada encaminador toma la decisión de encaminamiento basándose en el conocimiento que tiene sobre la topología y las condiciones de tráfico y retardo de las redes interconectadas. En un conjunto de redes sencillo, es posible utilizar un esquema de encaminamiento fijo. En conjuntos de redes más complejos, se necesita cierto grado de cooperación dinámica entre los dispositivos de encaminamiento o encaminadores. En particular, el encaminador debe evitar aquellas partes de la red que hayan sufrido una interrupción y debería evitar aquellas secciones de la red que sufran congestión. Para poder tomar estas decisiones de encaminamiento dinámicas, los encaminadores deben intercambiar información de encaminamiento mediante un protocolo de encaminamiento especial para ese propósito. Se necesita así información sobre el estado del conjunto de redes, en términos de qué redes son accesibles a través de qué dispositivos de encaminamiento, y las características de retardo de varias rutas.

Al considerar la función de encaminamiento, hay que distinguir dos conceptos:

- **Información de encaminamiento:** información sobre la topología y retardos del conjunto de redes interconectadas.
- **Algoritmo de encaminamiento:** algoritmo utilizado para la toma de decisiones de encaminamiento para un datagrama concreto, basado en la información de encaminamiento disponible.

SISTEMAS AUTÓNOMOS

Para continuar con nuestro análisis sobre los protocolos de encaminamiento, necesitamos introducir el concepto de **sistema autónomo**. Un sistema autónomo (AS, *Autonomous System*) posee las siguientes características:

1. Un AS se compone de un conjunto de encaminadores y redes gestionados por una única organización.
2. Un AS consiste en un grupo de dispositivos de encaminamiento que intercambian información a través de un protocolo de encaminamiento común.
3. Excepto en momentos de avería, un AS está conectado (en un sentido teórico de grafo). Es decir, existe un camino entre cualquier par de nodos.

Un protocolo común de encaminamiento, al que nos referiremos como **protocolo de encaminador interior** (IRP, *Interior Router Protocol*), distribuye la información de encaminamiento entre los dispositivos de encaminamiento dentro de un AS. El protocolo que se emplea dentro de un

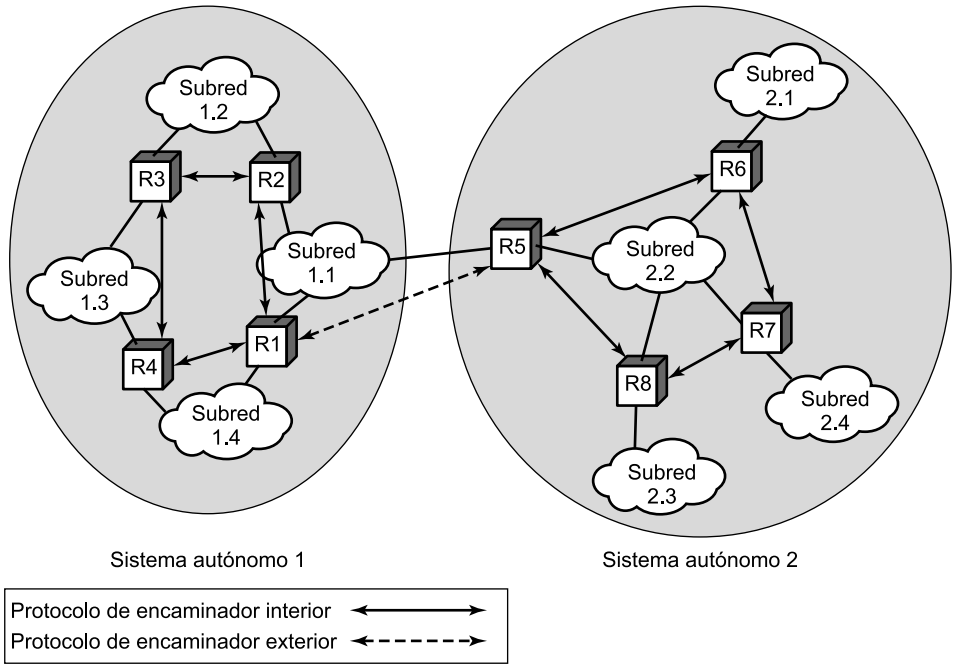


Figura 19.5. Aplicación de los protocolos de encaminamiento exterior e interior.

sistema autónomo no necesita ser implementado fuera del sistema. Esta flexibilidad permite que los IRP se hagan a medida para aplicaciones y requisitos específicos.

Puede ocurrir, sin embargo, que una interconexión de redes esté constituida por más de un AS. Por ejemplo, todas las LAN de una organización, como puede ser un complejo de oficinas o un campus, podrían estar enlazadas mediante encaminadores para formar un AS. Este sistema se podría unir a otros AS a través de una red de área amplia. Esta situación se muestra en la Figura 19.5. En este caso, los algoritmos de encaminamiento y la información de las tablas de encaminamiento utilizadas por los encaminadores en los distintos AS pueden ser diferentes. Sin embargo, los encaminadores de un AS necesitan al menos un nivel mínimo de información referente a las redes externas al sistema que puedan alcanzar. El protocolo que se utiliza para pasar información de encaminamiento entre diferentes AS se conoce como **protocolo de encaminador exterior** (ERP, *Exterior Router Protocol*)[3].

Podemos esperar que un ERP necesite pasar menos información que un IRP por la siguiente razón: si un datagrama va a ser transferido de una estación en un AS a una estación en otro AS, un encaminador del primer sistema sólo necesita determinar el AS objetivo y calcular una ruta para entrar en el sistema objetivo. Una vez que el datagrama entra en el AS destino, los encaminadores del sistema pueden cooperar para entregar el datagrama. El ERP no necesita conocer, y de hecho no conoce, los detalles de la ruta seguida en el AS destino.

[3] En la bibliografía relacionada se utilizan a menudo los términos *protocolo de pasarela interior* (IGP, *Interior Gateway Protocol*) y *protocolo de pasarela exterior* (EGP, *Exterior Gateway Protocol*) para designar lo que aquí denominamos IRP y ERP. Sin embargo, ya que los términos *IGP* y *EGP* también hacen referencia a protocolos concretos, evitaremos su uso para definir los conceptos generales.

En el resto de esta sección, examinaremos los que posiblemente sean los ejemplos más importantes de esos dos tipos de protocolos de encaminamiento: BGP y OSPF. Pero antes será útil examinar una forma diferente de caracterizar protocolos de encaminamiento.

ESTRATEGIAS DE ENCAMINAMIENTO

Los protocolos de encaminamiento para redes interconectadas emplean uno de estos tres enfoques para recopilar y utilizar la información de encaminamiento: encaminamiento por vector distancia, encaminamiento por estado de enlace y encaminamiento por vector camino.

El **encaminamiento por vector distancia** requiere que cada nodo (encaminador o estación que implemente el protocolo de encaminamiento) intercambie información con sus nodos vecinos. Dos nodos se consideran vecinos si están ambos directamente conectados a la misma red. Esta aproximación es la que se utilizó en la primera generación del algoritmo de encaminamiento para ARPANET, como se describe en la Sección 12.2. Para este fin, cada nodo mantiene un vector de costes por enlace para cada red directamente conectada y los vectores de distancia y de siguiente salto para cada destino. El relativamente simple protocolo de información de encaminamiento (RIP, *Routing Information Protocol*) utiliza este enfoque.

El encaminamiento por vector distancia requiere la transmisión de una considerable cantidad de información por parte de cada encaminador. Cada encaminador debe enviar un vector de distancias a todos sus vecinos. Ese vector contiene el costo estimado del camino a todas las redes de la configuración. Más aún, cuando se produce un cambio significativo en el coste de un enlace, o cuando un enlace no está disponible, la propagación de esta información a través de la red puede tomar una considerable cantidad de tiempo.

El **encaminamiento por estado de enlace** se diseñó para superar las deficiencias del encaminamiento de vector distancia. Cuando se inicializa un encaminador, éste determina el coste del enlace de cada una de sus interfaces de red. El encaminador anuncia este conjunto de costes de enlaces a todos los otros encaminadores de la topología de red, no sólo a los encaminadores vecinos. A partir de ese momento, el encaminador monitoriza los costes de sus enlaces. En cuanto hay un cambio significativo (el coste de un enlace se incrementa o disminuye sustancialmente, se crea un nuevo enlace o un enlace existente deja de estar disponible), el encaminador notifica otra vez su conjunto de costes de enlace a todos los dispositivos de encaminamiento de la configuración.

Dado que cada encaminador recibe los costes de los enlaces de todos los encaminadores de la configuración, cada encaminador puede construir la topología de toda la configuración y calcular después el camino más corto a cada red de destino. Una vez hecho esto, el encaminador puede construir su tabla de encaminamiento, listando el primer salto hacia cada destino. A diferencia del encaminamiento por vector distancia, el encaminador no utiliza una versión distribuida de un algoritmo de encaminamiento, ya que tiene una representación de toda la red. En su lugar, el encaminador puede utilizar cualquier algoritmo de encaminamiento para determinar los caminos mínimos. En la práctica se utiliza el algoritmo de Dijkstra. El protocolo del primer camino más corto disponible (OSPF) es un ejemplo de protocolo que emplea encaminamiento por estado de enlace. El algoritmo de encaminamiento de segunda generación para ARPANET emplea también esta estrategia.

Las aproximaciones de estado de enlace y vector distancia han sido empleadas para protocolos de encaminadores interiores. Ninguno de los dos enfoques es efectivo para un protocolo de encaminador exterior.

En el protocolo de encaminamiento por vector distancia, cada encaminador anuncia a sus vecinos un vector que lista las redes que puede alcanzar, junto a una medida de la distancia asociada a la ruta para esa red. Cada encaminador construye una base de datos de encaminamiento basada en las actualizaciones de los vecinos, pero desconoce la identidad de los encaminadores y redes intermedias de una ruta concreta. Con esta aproximación existen dos problemas para los protocolos de encaminadores exteriores:

1. Este protocolo de vector distancia supone que todos los encaminadores comparten una métrica de distancia común con la que juzgar las preferencias del encaminador. Éste puede no ser el caso entre diferentes AS. Si diferentes encaminadores asignan diferentes significados a una métrica dada, puede no ser posible crear rutas estables libres de bucles.
2. Un AS concreto puede tener diferentes prioridades con respecto a otros AS y puede tener restricciones que prohíban el uso de algún otro AS en concreto. Un algoritmo de vector distancia no da información sobre los AS que se visitarán a lo largo de la ruta.

En un protocolo de encaminamiento por estado de enlace, cada encaminador anuncia sus métricas de enlace a todos los otros encaminadores. Cada encaminador se construye una representación de la topología completa de la configuración y luego realiza un cálculo de encaminamiento. Este enfoque tiene también problemas si se utiliza en un protocolo de encaminador exterior:

1. Diferentes AS pueden utilizar diferentes métricas y tener diferentes restricciones. Aunque el protocolo de estado de enlace permite al encaminador construirse una imagen de la topología completa, las métricas utilizadas pueden variar de un AS a otro, haciendo imposible que se pueda llevar a cabo un algoritmo de encaminamiento consistente.
2. La inundación de la información de estado de enlace a todos los encaminadores que implementen un protocolo de encaminador exterior a través de distintos AS puede ser inmanejable.

Existe una alternativa, conocida como **encaminamiento por vector camino**, consistente en prescindir de métricas de encaminamiento y proporcionar simplemente información acerca de qué redes pueden ser alcanzadas por un encaminador determinado y los AS que se deben atravesar para llegar. Este enfoque se diferencia del algoritmo de vector distancia en dos aspectos: en primer lugar, la estrategia del vector camino no incluye una estimación de distancia o coste. En segundo lugar, cada bloque de información de encaminamiento enumera todos los AS visitados para alcanzar mediante esta ruta la red destino.

Debido a que un vector de camino enumera todos los AS que debe atravesar un datagrama si sigue esta ruta, la información del camino permite al encaminador llevar a cabo políticas de encaminamiento. Es decir, un encaminador puede decidir evitar un camino determinado para evitar transitar por un AS concreto. Por ejemplo, una información confidencial puede ser limitada a ciertas clases de AS, o un encaminador puede tener información acerca del rendimiento o calidad de la porción de la red que esté incluida en un AS, lo que le lleva al encaminador a evitar dicho AS. Ejemplos de métricas de rendimiento o de calidad incluyen la velocidad del enlace, la capacidad, la tendencia a congestionarse y la calidad global de funcionamiento. Otro criterio que podría utilizarse es minimizar el número AS transitados.

PROTOCOLO DE PASARELA FRONTERA

El protocolo de pasarela frontera (BGP, *Border Gateway Protocol*) se desarrolló para su uso en conjunción con interconexiones de redes que empleen la arquitectura de protocolos TCP/IP, aun-

que los conceptos son aplicables a cualquier interconexión de redes. BGP se ha convertido en el protocolo de dispositivo de encaminamiento exterior preferido para Internet.

Funciones

BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento de diferentes sistemas autónomos (AS), llamados pasarelas en el estándar. El protocolo opera en términos de mensajes, que se envían utilizando conexiones TCP. El repertorio de mensajes se resume en la Tabla 19.2. La versión actual de BGP se conoce como BGP-4 (RFC 1771).

Tabla 19.2. Mensajes de BGP-4.

Establecer	Utilizado para establecer una relación de vecindad con otro dispositivo de encaminamiento.
Actualizar	Utilizado para (1) transmitir información acerca de una única ruta y/o (2) enumerar rutas múltiples que se vayan a eliminar.
Mantener activa	Utilizado para (1) confirmar un mensaje «establecer» y (2) confirmar periódicamente la relación de vecindad.
Notificación	Se envía cuando se detecta una condición de error.

BGP supone tres procedimientos funcionales, que son:

- Adquisición de vecino.
- Detección de vecino alcanzable.
- Detección de red alcanzable.

Dos dispositivos de encaminamiento se considera que son vecinos si están conectados a la misma subred. Si los dos encaminadores se encuentran en sistemas autónomos diferentes, podrían desear intercambiar información de encaminamiento. Para este cometido, es necesario primero realizar la operación de **adquisición de vecino**. Básicamente, la adquisición de un vecino se produce cuando dos dispositivos de encaminamiento vecinos de diferentes sistemas autónomos se ponen de acuerdo en intercambiar regularmente información de encaminamiento. Se requiere un procedimiento formal de adquisición debido a que uno de los encaminadores podría no querer participar. Por ejemplo, el dispositivo de encaminamiento puede estar sobresaturado y no querer ser responsable de tráfico que llegue de fuera del sistema. En el proceso de adquisición de un vecino, un dispositivo de encaminamiento envía un mensaje de petición al otro, el cual puede aceptar o rechazar el ofrecimiento. El protocolo no aborda la cuestión de cómo puede un dispositivo de encaminamiento conocer la dirección o incluso la existencia de otro encaminador, ni siquiera de cómo decide que necesita intercambiar información de encaminamiento con un encaminador en particular. Estas cuestiones deben ser tratadas en el momento de establecer la configuración o mediante una intervención activa del administrador de la red.

Para llevar a cabo la adquisición de vecino, un dispositivo de encaminamiento envía a otro un mensaje «establecer» («*Open*»). Si el encaminador destino acepta la solicitud, devuelve un mensaje «mantener activa» («*Keepalive*») como respuesta.

Una vez establecida la relación de vecino, se utiliza el procedimiento **detección de vecino alcanzable** para mantener la relación. Cada asociado necesita estar seguro de que el otro asociado

existe y está todavía comprometido con la relación de vecino. Con este propósito, ambos dispositivos de encaminamiento se envían periódicamente mensajes «mantener activa».

El último procedimiento especificado por BGP es la **detección de red alcanzable**. Cada dispositivo de encaminamiento mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para ello. Siempre que se produzca un cambio en esta base de datos, el dispositivo de encaminamiento difunde un mensaje «actualizar» («*Update*») a todos los otros dispositivos de encaminamiento que implementen BGP. Dado que el mensaje «actualizar» se envía por difusión, todos los encaminadores BGP pueden generar y mantener su información de encaminamiento.

Mensajes BGP

La Figura 19.6 muestra el formato de todos los mensajes BGP. Cada mensaje comienza con una cabecera de 19 bytes que contiene tres campos, como se indica en la parte sombreada en la figura:

- **Marcador:** reservado para autenticación. El emisor puede insertar un valor en este campo que se emplearía como parte de un mecanismo de autenticación para permitir al destino verificar la identidad del emisor.
- **Longitud:** longitud del mensaje en bytes.
- **Tipo:** tipo de mensaje: establecer, actualizar, notificación o mantener activa.

Para adquirir un vecino, un encaminador abre primero una conexión TCP con el encaminador vecino de interés. Entonces envía un mensaje «establecer». Este mensaje identifica al AS al que pertenece el emisor y proporciona la dirección IP del dispositivo de encaminamiento. También incluye un parámetro de tiempo de mantenimiento, que indica el número de segundos que propone el emisor para el temporizador de mantenimiento. Si el destino está preparado para establecer una relación de vecindad, calcula un valor para el temporizador de mantenimiento como el mínimo entre su tiempo de mantenimiento y el valor de tiempo especificado en el mensaje «establecer». El valor calculado representa el máximo número de segundos que pueden transcurrir entre la recepción en el emisor de mensajes «mantener activa» sucesivos y/o mensajes «actualizar».

El mensaje «mantener activa» consta sólo de la cabecera. Cada dispositivo de encaminamiento emite estos mensajes a cada uno de sus pares con suficiente regularidad para evitar que expire su temporizador de mantenimiento.

El mensaje «actualizar» facilita dos tipos de información:

- Información sobre una ruta determinada a través de la interconexión de redes. Esta información se puede incorporar a la base de datos de cualquier dispositivo de encaminamiento que la recibe.
- Una lista de rutas previamente anunciadas por este dispositivo de encaminamiento que van a ser eliminadas.

Un mensaje «actualizar» puede contener uno o ambos tipos de información. La información sobre una ruta particular a través de la red incluye tres campos: el campo de información de alcanzabilidad de la capa de red (NLRI, *Network Layer Reachability Information*), el campo de longitud total de los atributos de la ruta y el campo de los atributos de la ruta. El campo NLRI contiene una lista de identificadores de redes que se pueden alcanzar por esta ruta. Cada red se identifica por su dirección IP, que es en realidad una parte de una dirección IP completa. Recuerde que una dirección IP es una cantidad de 32 bits de la forma {red, estación}. El prefijo o parte izquierda de esta cantidad identifica a una red concreta.

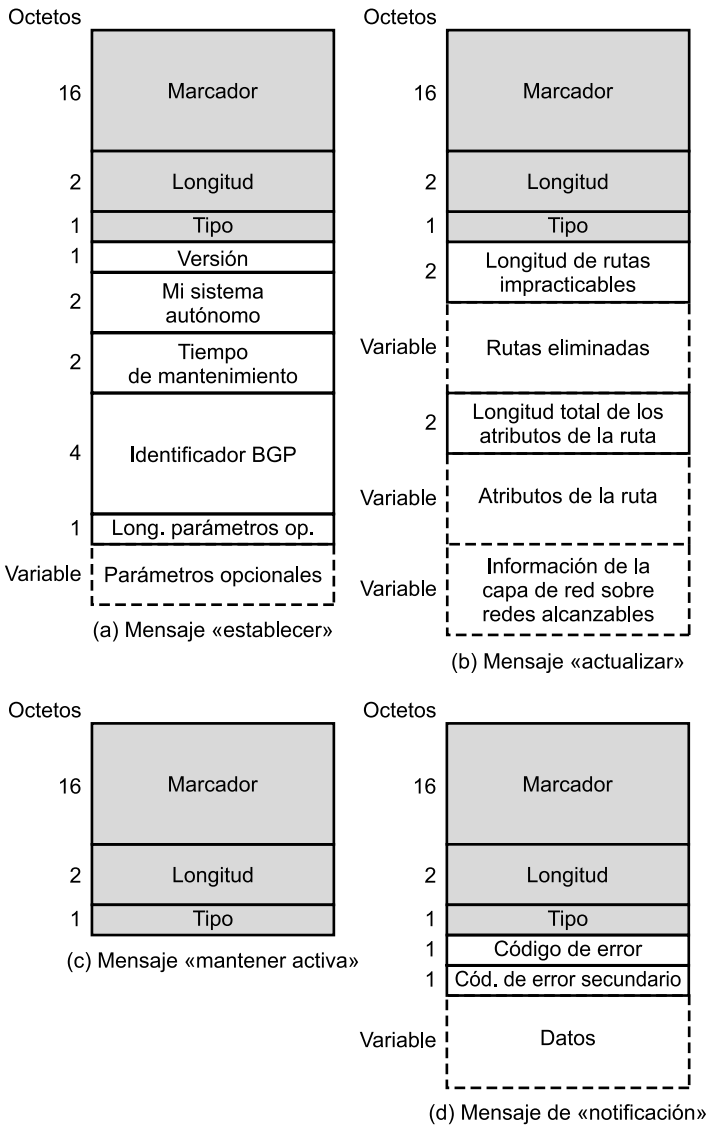


Figura 19.6. Formatos de los mensajes BGP.

El campo atributos de la ruta contiene una lista de atributos que se aplican a esta ruta concreta. Los atributos definidos son los siguientes:

- **Origen:** indica si la información fue generada por un protocolo de dispositivo de encaminamiento interior (por ejemplo, OSPF) o por un protocolo de dispositivo de encaminamiento exterior (en particular, BGP).
- **Camino AS:** una lista de los AS que son recorridos por la ruta.
- **Siguiente salto:** dirección IP del dispositivo de encaminamiento frontera que se debe usar como siguiente salto para alcanzar los destinos indicados en el campo NLRI.

- **Discriminante de salida múltiple:** se emplea para comunicar alguna información sobre rutas internas a un AS. Este atributo se describirá más adelante en esta sección.
- **Preferencias locales:** empleado por un dispositivo de encaminamiento para informar a otros dispositivos de encaminamiento de su mismo AS de su grado de preferencia por una ruta particular. No tiene significado alguno para los dispositivos de encaminamiento de otros AS.
- **Agregado atómico, Agente unión (*Atomic_aggregate, Aggregator*):** estos dos campos implementan el concepto de unión de rutas. En esencia, un conjunto de redes interconectadas y su espacio de direcciones correspondiente se pueden organizar jerárquicamente (es decir, como un árbol). En este caso, las direcciones de las redes se estructuran en dos o más partes. Todas las redes de un subárbol comparten una dirección de red parcial común. Usando esta dirección parcial común, la cantidad de información que se debe comunicar en el campo NLRI se puede reducir significativamente.

El atributo «camino AS» sirve realmente para dos objetivos. Dado que indica los AS que debe atravesar un datagrama si sigue esta ruta, la información de camino AS permite a un dispositivo de encaminamiento implementar políticas de encaminamiento. Es decir, un dispositivo de encaminamiento puede decidir evitar un camino particular para evitar el paso por un AS concreto. Por ejemplo, la información que es confidencial puede estar limitada a ciertos tipos de AS, o un encaminador puede tener información sobre el rendimiento o calidad de una porción de red que esté incluida en un AS, lo que lleva al encaminador evitar ese AS. Algunos ejemplos de rendimiento o métrica de calidad son: velocidad del enlace, la capacidad, la tendencia a estar congestionado y la calidad global de funcionamiento. Otro criterio que se podría usar es minimizar el número de AS de tránsito.

El lector se puede preguntar por el objetivo del atributo siguiente salto. El dispositivo de encaminamiento que realiza la solicitud querrá conocer necesariamente qué redes se pueden alcanzar a través del encaminador que responde pero, ¿por qué proporcionar información acerca de otros dispositivos de encaminamiento? Esta cuestión se explica mejor con la ayuda de la Figura 19.5. En este ejemplo, el dispositivo de encaminamiento R1 en el sistema autónomo 1 y el dispositivo de encaminamiento R5 en el sistema autónomo 2 implementan BGP y establecen una relación de vecindad. R1 envía un mensaje «actualizar» a R5 indicando qué redes puede alcanzar y las distancias (saltos de red) implicadas. R1 también proporciona la misma información en representación de R2. Es decir, R1 le dice a R5 qué redes se pueden alcanzar vía R2. En este ejemplo, R2 no implementa BGP. Normalmente, la mayoría de los dispositivos de encaminamiento en un sistema autónomo no implementan BGP. Sólo unos pocos dispositivos de encaminamiento tendrán asignada la responsabilidad de comunicarse con otros encaminadores de otros sistemas autónomos. Un apunte final: R1 tiene la información necesaria sobre R2 debido a que R1 y R2 comparten un protocolo de encaminador interior (IRP).

El segundo tipo de información de actualización consiste en la supresión de una o más rutas. En este caso, la ruta se identifica por la dirección IP de la red destino.

Finalmente, el mensaje de «notificación» se envía cuando se detecta una condición de error. Se puede informar de los siguientes errores:

- **Error en la cabecera del mensaje:** incluye errores de sintaxis y de autenticación.
- **Error en un mensaje «establecer»:** incluye errores de sintaxis y opciones no reconocidas en un mensaje «establecer». Este mensaje también se puede utilizar para indicar que el tiempo de mantenimiento en un mensaje «establecer» es inaceptable.
- **Error en un mensaje «actualizar»:** incluye errores de sintaxis y validez en un mensaje «actualizar».

- **Tiempo de mantenimiento expirado:** Si el dispositivo de encaminamiento emisor no ha recibido sucesivos mensajes «mantener activa» y/o «actualizar» y/o mensajes de «notificación» durante el tiempo de mantenimiento, entonces se comunica este error y se cierra la conexión.
- **Error en la máquina de estados finitos:** Incluye cualquier error de procedimiento.
- **Cese:** Utilizado por un dispositivo de encaminamiento para cerrar una conexión con otro encaminador en ausencia de cualquier otro error.

Intercambio de información de encaminamiento de BGP

La esencia de BGP es el intercambio de información de encaminamiento entre dispositivos de encaminamiento participantes en múltiples AS. Este proceso puede ser bastante complejo. A continuación, proporcionaremos una visión simplificada.

Consideremos el dispositivo de encaminamiento R1 en el sistema autónomo 1 (AS1) de la Figura 19.5. Para empezar, un encaminador que implemente BGP implementará también un protocolo encaminamiento interno como OSPF. Usando OSPF, R1 puede intercambiar información de encaminamiento con otros dispositivos de encaminamiento dentro de AS1 y construir un esquema de la topología de las redes y dispositivos de encaminamiento en AS1 para construir una tabla de encaminamiento. A continuación, R1 puede emitir un mensaje «actualizar» a R5 en AS2. El mensaje «actualizar» podría incluir lo siguiente:

- **Camino AS:** la identidad de AS1.
- **Siguiente salto:** la dirección IP de R1.
- **NLRI:** una lista de todas las redes de AS1.

Este mensaje informa a R5 que todas las redes indicadas en NLRI se alcanzan vía R1 y que el único sistema autónomo que hay que atravesar es AS1.

Suponga ahora que R5 también mantiene una relación de vecindad con otro dispositivo de encaminamiento en otro sistema autónomo, digamos R9 en AS3. R5 enviará la información que acaba de recibir de R1 a R9 en un nuevo mensaje «actualizar». Este mensaje incluye lo siguiente:

- **Camino AS:** la lista de identificadores {AS2, AS1}.
- **Siguiente salto:** la dirección IP de R5.
- **NLRI:** una lista de todas las redes en AS1.

Este mensaje informa a R9 de que todas las redes indicadas en NLRI son alcanzables vía R5 y que los sistemas autónomos que hay que atravesar son AS2 y AS1. R9 debe decidir si ésta es ahora su ruta preferida hacia las redes indicadas. R9 podría conocer una ruta alternativa a alguna o a todas esas redes, prefiriéndola por razones de rendimiento o algún otro criterio métrico. Si R9 decide que la ruta proporcionada en el mensaje de actualización de R5 es preferible, entonces incorpora la información de encaminamiento en su base de datos de encaminamiento y propaga la nueva información a otros vecinos. Este mensaje nuevo incluirá un campo camino AS del tipo {AS3, AS2, AS1}.

De esta forma, la información de encaminamiento de actualización se propaga a través de la interconexión de redes mayor, que consta a su vez de varios sistemas autónomos interconectados. El campo camino AS se emplea para asegurar que el mensaje no circula indefinidamente: si un

dispositivo de encaminamiento recibe un mensaje «actualizar» en un AS que esté incluido en el campo camino AS, ese encaminador no enviará la información de actualización a otros encaminadores.

Los dispositivos de encaminamiento de un mismo AS, denominados vecinos internos, pueden intercambiar información BGP. En este caso, el dispositivo de encaminamiento emisor no incorpora el identificador del AS común al campo camino AS. Cuando un encaminador ha seleccionado una ruta a un destino externo como preferida, transmite esta ruta a todos sus vecinos internos. Cada uno de estos dispositivos de encaminamiento decide entonces si la nueva ruta pasa a ser la preferida, en cuyo caso incorpora la nueva ruta a su base de datos y envía un nuevo mensaje «actualizar».

Cuando hay disponibles múltiples puntos de entrada a un AS desde un dispositivo de encaminamiento fronterizo de otro AS, el atributo discriminante de salida múltiple puede utilizarse para elegir uno de ellos. Este atributo contiene un número que refleja alguna métrica interna para alcanzar los destinos dentro de un AS. Por ejemplo, suponga que en la Figura 19.5 los dispositivos de encaminamiento R1 y R2 implementan BGP, y que ambos tienen una relación de vecindad con R5. Cada uno envía un mensaje «actualizar» a R5 para la red 1.3 que incluye una métrica de encaminamiento utilizada internamente en AS1, al igual que la métrica de encaminamiento asociada con el protocolo de encaminador interno OSPF. R5 podría usar entonces estas dos métricas nuevas como criterio para elegir entre las dos rutas.

PROTOCOLO DEL PRIMER CAMINO MÁS CORTO DISPONIBLE

El protocolo del primer camino más corto disponible (OSPF, *Open Shortest Path First*, RFC 2328) se usa de forma generalizada como protocolo de encaminador interior en redes TCP/IP. OSPF calcula una ruta a través de una interconexión de redes que suponga el menor coste de acuerdo a una métrica de coste configurable por usuario. El usuario puede configurar el coste para que exprese una función del retardo, la velocidad de transmisión, el coste económico u otros factores. OSPF es capaz de equilibrar las cargas entre múltiples caminos de igual coste.

Cada dispositivo de encaminamiento mantiene una base de datos que refleja la topología conocida del sistema autónomo del que forma parte. Esta topología se expresa como un grafo dirigido. El grafo consta de:

- Vértices o nodos, de dos tipos:
  1. Dispositivo de encaminamiento;
  2. Red, que también puede ser de dos tipos:
     a) De tránsito, si pueden transportar datos que no se han originado ni van dirigidos a un sistema final conectado a esta red;
     b) Terminal, si no es una red de tránsito.
- Arcos, de dos tipos:
  1. Arcos del grafo que conectan dos vértices de encaminadores cuando los dispositivos de encaminamiento correspondientes están conectados el uno al otro mediante un enlace directo punto a punto.
  2. Arcos del grafo que conectan un vértice de encaminador a un vértice de red cuando el encaminador está directamente conectado a la red.

La Figura 19.7, basada en una figura del RFC 2328, muestra un ejemplo de un sistema autónomo y la Figura 19.8 el correspondiente grafo dirigido. La correspondencia es sencilla:

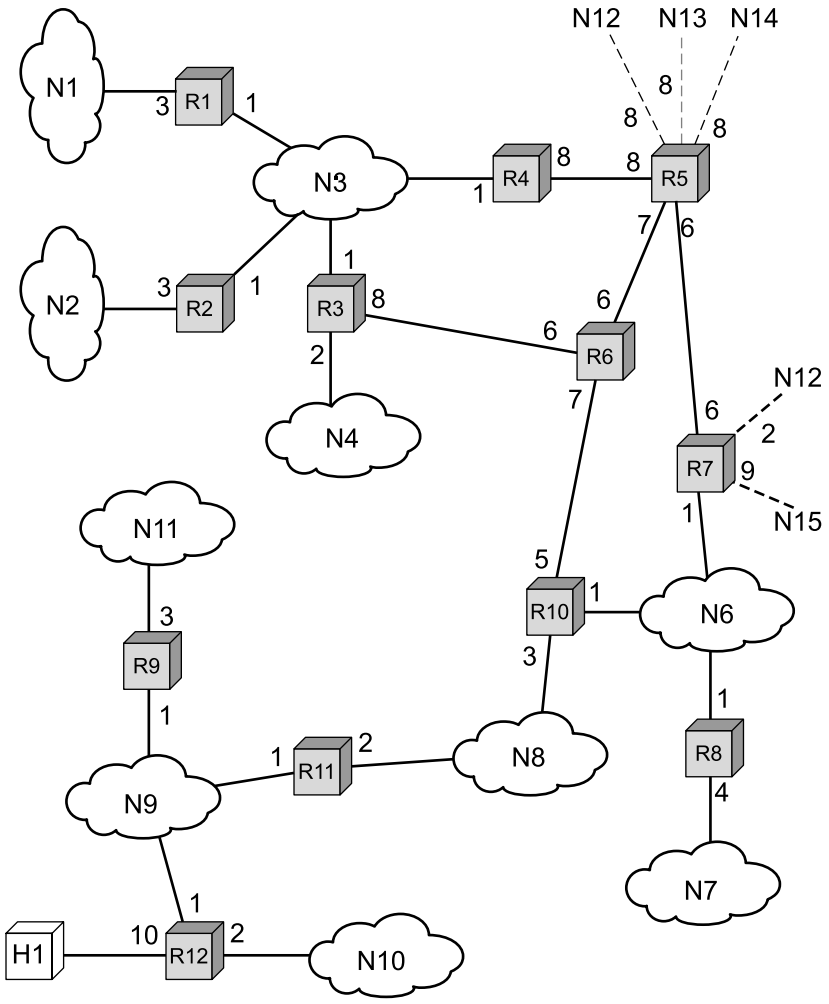


Figura 19.7. Ejemplo de sistema autónomo.

- Dos dispositivos de encaminamiento unidos por un enlace punto a punto están representados en el grafo mediante una conexión directa por dos arcos, uno en cada sentido (por ejemplo, los encaminadores 6 y 10).
- Cuando varios dispositivos de encaminamiento están conectados a una red (como una LAN o una red de conmutación de paquetes), el grafo dirigido muestra a todos los dispositivos de encaminamiento conectados en los dos sentidos al vértice de red (por ejemplo, los encaminadores 1, 2, 3 y 4, todos conectados a la red 3).
- Si un único dispositivo de encaminamiento está conectado a una red, la red aparecerá en el grafo como una conexión terminal (por ejemplo, la red 7).
- Un sistema final, denominado estación, se puede conectar directamente a un dispositivo de encaminamiento, en cuyo caso se dibuja en el grafo correspondiente (por ejemplo, la estación 1).

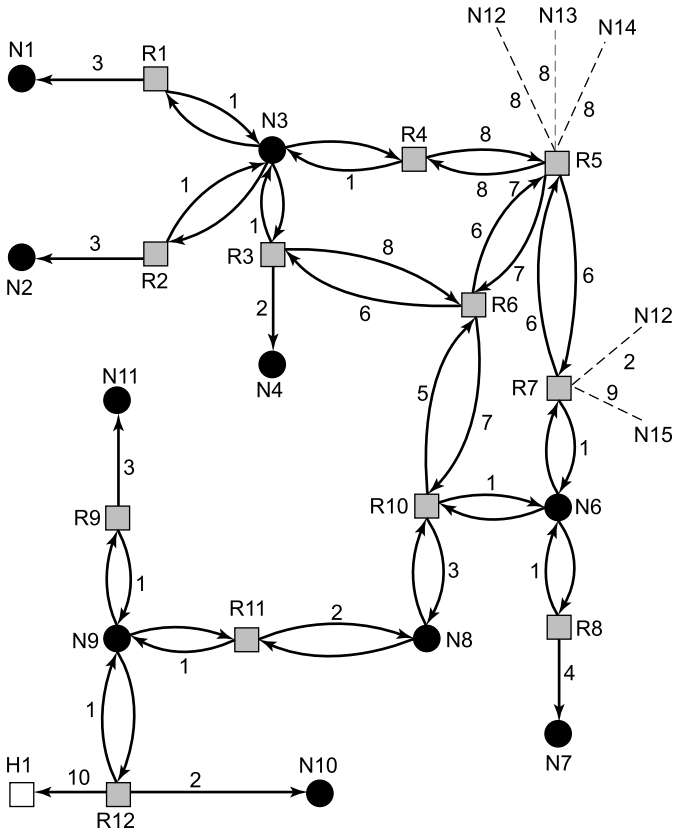


Figura 19.8. Grafo dirigido del sistema autónomo de la Figura 19.7.

- Si un dispositivo de encaminamiento está conectado a otros sistemas autónomos, entonces el coste del camino a cada una de las redes en el otro sistema debe obtenerse mediante algún protocolo de encaminador exterior (ERP). Cada una de estas redes se representa en el grafo por una red terminal y un arco al encaminador con el coste conocido del camino (por ejemplo, las redes 12 a la 15).

A cada salida de cada interfaz de los encaminadores se le asocia un coste. Este coste es configurable por el administrador del sistema. Los arcos en el grafo se etiquetan con el coste de la interfaz de salida del dispositivo de encaminamiento correspondiente. Los arcos que no tienen etiqueta tienen un coste 0. Observe que los arcos que van de las redes a los dispositivos de encaminamiento tienen siempre coste 0.

En cada dispositivo de encaminamiento se mantiene una base de datos correspondiente al grafo dirigido. Se reconstruye mediante los mensajes de estado del enlace provenientes de otros encaminadores de la interconexión de redes. Un dispositivo de encaminamiento calcula el camino de menor coste a todas las redes destino usando el algoritmo de Dijkstra (*véase* la Sección 12.3). El resultado para el encaminador 6 de la Figura 19.7 se muestra como un árbol en la Figura 19.9, con R6 como raíz del árbol. El árbol da la ruta completa a cualquier red o estación destino. Sin embargo, sólo se usa el siguiente salto para el proceso de reenvío. La tabla de encaminamiento resultante para el dispositivo de encaminamiento 6 se muestra en la Tabla 19.3. Ésta incluye entradas para los

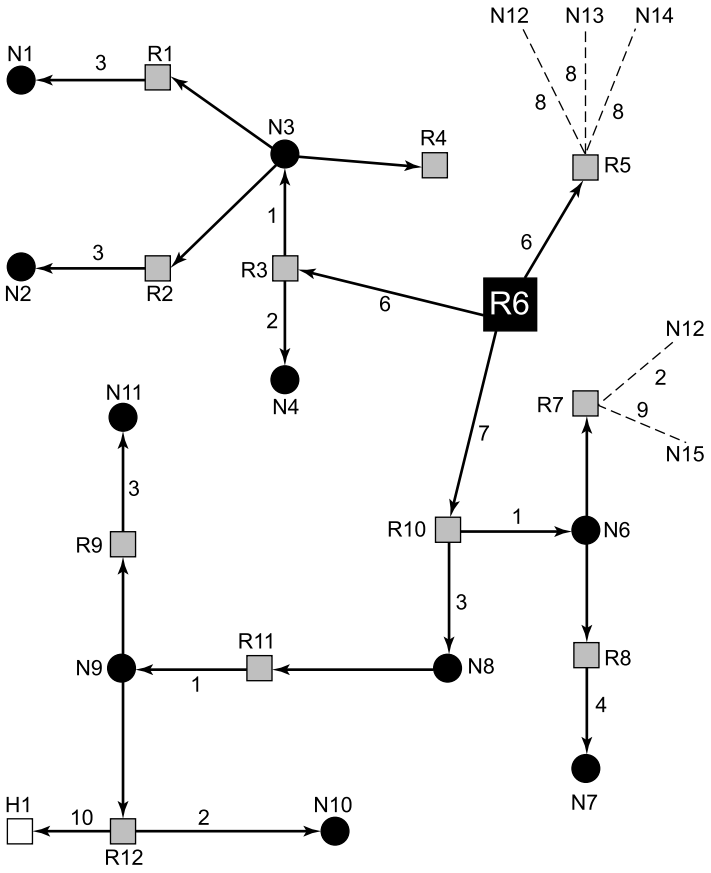


Figura 19.9. Árbol SPF para el encaminador R6.

encaminadores que informan de rutas externas (dispositivos de encaminamiento 5 y 7). También se proporcionan entradas para las redes externas cuya identidad se conozca.

19.3. ARQUITECTURA DE SERVICIOS INTEGRADOS

Para satisfacer los requisitos del servicio de QoS, la IETF está desarrollando un conjunto de estándares bajo el paraguas general de la arquitectura de servicios integrados (ISA, *Integrated Services Architecture*). ISA, cuya finalidad es la de proporcionar transporte con QoS sobre interconexiones de redes basadas en IP, se define en términos generales en el RFC 1633, mientras que se están desarrollando otros documentos para completar los detalles. De hecho, varios fabricantes han implementado partes de ISA en encaminadores y software de sistemas finales.

Esta sección ofrece una visión general de ISA.

TRÁFICO EN INTERNET

El tráfico existente en una red o interconexión de redes se puede dividir en dos categorías generales: tráfico elástico y tráfico inelástico. Una consideración de sus diferentes requisitos clarifica la necesidad de una arquitectura de red mejorada.

Tabla 19.3. Tabla de encaminamiento para R6.

Destino	Siguiente salto	Distancia
N1	R3	10
N2	R3	10
N3	R3	7
N4	R3	8
N6	R10	8
N7	R10	12
N8	R10	10
N9	R10	11
N10	R10	13
N11	R10	14
H1	R10	21
R5	R5	6
R7	R10	8
N12	R10	10
N13	R5	14
N14	R5	14
N15	R10	17

Tráfico elástico

El tráfico elástico es aquel que se puede ajustar, sobre un amplio margen, a cambios en el retardo y rendimiento experimentados a través de un conjunto de redes interconectadas y aun así satisfacer las necesidades de sus aplicaciones. Éste es el tipo tradicional de tráfico soportado por las redes basadas en TCP /IP y es el tipo de tráfico para el cual se diseñaron las interconexiones de redes. Las aplicaciones que generan este tráfico normalmente utilizan TCP o UDP como protocolo de transporte. En el caso de UDP, la aplicación utilizará tanta capacidad como haya disponible, con el límite que imponga la velocidad de la aplicación que genera los datos. En el caso de TCP, la aplicación utilizará tanta capacidad como haya disponible hasta un máximo correspondiente a la velocidad de datos que el receptor puede aceptar. Además, con TCP, el tráfico en las conexiones individuales se ajusta a la congestión reduciendo la velocidad a la que se envían los datos por la red. Este caso se describe en el Capítulo 20.

Las aplicaciones que se pueden clasificar como elásticas comprenden las aplicaciones comunes que funcionan sobre TCP o UDP, entre ellas la transferencia de ficheros (FTP), el correo electrónico (SMTP), la conexión remota (TELNET), la gestión de red (SNMP) y el acceso a la información web (HTTP). Sin embargo, existen diferencias entre las necesidades de estas aplicaciones. Por ejemplo:

- El correo electrónico es generalmente bastante insensible a los cambios en el retardo.
- Cuando la transferencia de ficheros se hace de forma interactiva, y es así normalmente, el usuario espera que el retardo sea proporcional al tamaño del fichero y, por tanto, es sensible a cambios en el rendimiento.
- Para la gestión de red, el retardo no es en general un asunto preocupante. Sin embargo, si los fallos en una red son la causa de la congestión, entonces la necesidad de que los mensajes SNMP se envíen con un retardo mínimo aumenta con la congestión.

- Las aplicaciones interactivas, como la conexión remota y el acceso web, son bastantes sensibles al retardo.

Es importante comprender que no es el retardo de cada paquete la medida de interés. Como se indica en [CLAR95], la observación de retardos reales a través de Internet indica que no se experimentan grandes variaciones en el retardo. Debido a los mecanismos de control de congestión de TCP, cuando aparece congestión, los retardos sólo se incrementan de forma moderada antes de que la velocidad de llegada de datos de las conexiones TCP disminuya. En cambio, la QoS percibida por el usuario se corresponde con el tiempo total transcurrido para transferir un elemento de la aplicación en curso. Para una aplicación basada en TELNET interactivo, el elemento puede consistir en la pulsación de una tecla o en una sola línea. Para el acceso web, el elemento puede consistir en una página web, que puede tener un tamaño de sólo unos pocos kilobytes, o puede ser sustancialmente más grande en el caso de una página rica en imágenes. Para una aplicación científica, el elemento podría consistir en varios megabytes de datos.

Para elementos muy pequeños, el tiempo total transcurrido está dominado por el tiempo de retardo experimentado a través de la red. Sin embargo, para elementos de mayor tamaño, el tiempo total transcurrido lo dicta el comportamiento de la ventana deslizante de TCP y, por tanto, está dominado por el rendimiento alcanzado en la conexión TCP. De esta forma, para transferencias de gran volumen, el tiempo de transferencia es proporcional al tamaño del fichero y al grado en que la fuente reduce el envío debido a la congestión.

Debe quedar claro que aunque centráramos nuestra atención sólo en el tráfico elástico, un servicio de red basado en QoS podría ser beneficioso. Sin este tipo de servicio, los dispositivos de encaminamiento tratan imparcialmente los paquetes IP que reciben, sin preocuparse del tipo de aplicación ni de si un paquete en particular es parte de un elemento de transferencia voluminoso o pequeño. Bajo tales circunstancias, y si aparece la congestión, no es probable que los recursos se asignen de tal forma que se satisfagan las necesidades de todas las aplicaciones de forma equitativa. Cuando se añade tráfico inelástico a la mezcla, los resultados son incluso más insatisfactorios.

Tráfico inelástico

El tráfico inelástico no se adapta fácilmente, si es que lo hace, a los cambios en el retardo y el rendimiento que se experimentan en una interconexión de redes. El principal ejemplo lo constituye el tráfico en tiempo real. Las necesidades del tráfico inelástico son algunas de las siguientes:

- **Rendimiento:** se puede requerir un valor mínimo de rendimiento. A diferencia de la mayoría del tráfico elástico, que puede continuar entregando datos con tal vez un servicio degradado, muchas aplicaciones inelásticas requieren un estricto rendimiento mínimo dado.
- **Retardo:** un ejemplo de aplicación sensible al retardo es el negociado de las acciones en bolsa. Alguien que reciba sistemáticamente un servicio tardío actuará consecuentemente tarde y con una mayor desventaja.
- **Dispersión temporal:** la magnitud de variación del retardo, llamada dispersión del retardo (*jitter*), es un factor crítico en las aplicaciones de tiempo real. Cuanto mayor es la variación del retardo permitida, mayor es el retardo real para entregar los datos y más grande es el tamaño de la memoria temporal necesaria en los receptores. Las aplicaciones interactivas en tiempo real, como es el caso de la teleconferencia, pueden requerir un límite superior razonable para la variación del retardo.

- **Pérdida de paquetes:** las aplicaciones en tiempo real difieren en la cantidad de paquetes perdidos que pueden tolerar, si es que pueden afrontar pérdida de paquetes.

Estos requisitos son difíciles de satisfacer en un entorno con retardos de cola y pérdidas debidas a congestión variables. Por tanto, el tráfico inelástico introduce dos nuevos requisitos en la arquitectura de interconexión de redes. Primero, se necesitan medios para dar un tratamiento preferente a las aplicaciones con requisitos más exigentes. Las aplicaciones deben ser capaces de declarar sus necesidades, bien con antelación mediante algún tipo de función de solicitud de servicio, o bien en el momento, por medio de campos en la cabecera del paquete IP. La primera propuesta proporciona una mayor flexibilidad a la hora de indicar las necesidades y permite a la red anticipar demandas y denegar nuevas solicitudes si los recursos solicitados no están disponibles. Esta propuesta implica el uso de algún tipo de protocolo de reserva de recursos.

Como segundo requisito en la provisión de servicios para dar soporte al tráfico inelástico en una arquitectura de interconexión de redes, el tráfico elástico se debe seguir atendiendo. Las aplicaciones inelásticas no decaen ni reducen su demanda cuando se enfrentan a la congestión, a diferencia de las aplicaciones basadas en TCP. Por tanto, en los periodos de congestión, el tráfico inelástico continuará suministrando una carga elevada y el tráfico elástico será retirado de la red. Un protocolo de reserva puede ayudar a controlar esta situación denegando las solicitudes de servicio que, de otra forma, dejarían muy pocos recursos disponibles para tratar el tráfico elástico actual.

ENFOQUE ISA

El propósito de ISA es habilitar la provisión de soporte a QoS en una interconexión de redes IP. La principal cuestión de diseño en ISA consiste en cómo compartir la capacidad disponible en periodos de congestión.

Para un conjunto de redes interconectadas basadas en IP que sólo proporcionen un servicio de mejor esfuerzo, las herramientas para controlar la congestión y proporcionar servicios son limitadas. Básicamente, los dispositivos de encaminamiento tienen dos mecanismos para actuar:

- **Algoritmo de encaminamiento:** La mayoría de los protocolos de encaminamiento en uso en redes interconectadas permiten elegir rutas que minimicen el retardo. Los dispositivos de encaminamiento intercambian información para obtener una representación de los retardos a través del conjunto de redes. El encaminamiento de mínimo retardo ayuda a balancear la carga, disminuyendo así la congestión local, y también a reducir los retardos experimentados por las conexiones TCP individuales.
- **Descarte de paquetes:** Cuando la memoria temporal de un dispositivo de encaminamiento se agota, éste descarta paquetes. Normalmente, se descarta el paquete más reciente. El efecto de la pérdida de paquetes en una conexión TCP es que la entidad TCP que envía reduce su carga a la red, ayudando a aliviar de esta forma la congestión de la red.

Estas herramientas han funcionado razonablemente bien. Sin embargo, como muestra la discusión de la sección anterior, estas técnicas son inadecuadas para la diversidad de tráfico de red venidero.

ISA es una arquitectura global dentro de la que se están desarrollando una serie de mejoras sobre el tradicional mecanismo de mejor esfuerzo. En ISA, cada paquete IP se puede asociar con un flujo. El RFC 1633 define un flujo como una sucesión distinguible de paquetes IP relacionados que provengan de una única actividad de usuario y que requieran la misma QoS. Por ejemplo, un flujo podría estar compuesto por una conexión de transporte o un flujo de vídeo distinguible por ISA. Un flujo se diferencia de una conexión TCP en dos detalles clave: un flujo es unidireccional y

puede tener más de un destino (multidifusión). Normalmente, un paquete IP se identifica como miembro de un flujo mediante las direcciones IP origen y destino, los números de puerto y el tipo de protocolo. El identificador de flujo de la cabecera IPv6 no es necesariamente equivalente a un flujo ISA, pero en el futuro el identificador de flujo de IPv6 se podría utilizar en ISA.

ISA hace uso de las funciones siguientes para controlar la congestión y proporcionar transporte con QoS:

- **Control de admisión:** para el transporte con QoS (aparte del transporte de mejor esfuerzo que se tiene por defecto), ISA requiere que se haga una reserva para cada flujo nuevo. Si los dispositivos de encaminamiento determinan colectivamente que no hay suficientes recursos para garantizar la QoS solicitada, entonces el flujo no se admite. El protocolo RSVP se utiliza para hacer las reservas.
- **Algoritmo de encaminamiento:** la decisión de encaminamiento puede estar basada en diversos parámetros de QoS, no solamente en el mínimo retardo. Por ejemplo, el protocolo de encaminamiento OSPF, discutido en la Sección 19.2, puede seleccionar rutas basándose en su QoS.
- **Disciplinas de atención de cola:** un elemento vital de ISA es una política de atención de cola efectiva que tenga en cuenta las diferentes necesidades de los diferentes flujos.
- **Política de descarte:** una política de descarte determina qué paquete se ha de descartar cuando una memoria temporal esté llena y lleguen nuevos paquetes. Una política de descarte puede ser un elemento importante para gestionar la congestión y satisfacer la QoS garantizada.

COMPONENTES ISA

La Figura 19.10 muestra un diagrama general de la arquitectura de implementación para ISA en un dispositivo de encaminamiento. Bajo la línea horizontal gruesa se encuentran las funciones de reenvío del encaminador. Éstas se ejecutan para cada paquete y, por tanto, deben estar altamente optimizadas. El resto de funciones, por encima de la línea, son funciones secundarias que crean estructuras de datos utilizadas por las funciones de reenvío.

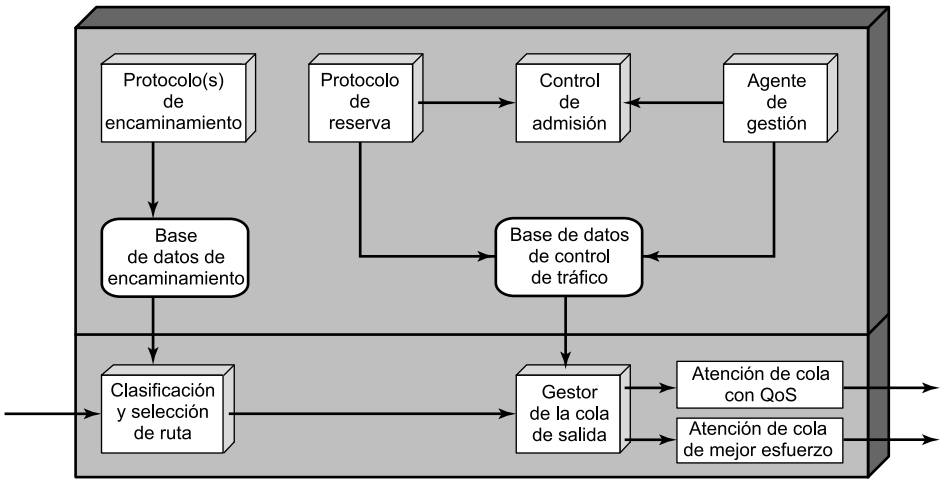

Protocolo(s) de encaminamiento
Protocolo de reserva
Control de admisión
Agente de gestión
Base de datos de encaminamiento
Base de datos de control de tráfico
Clasificación y selección de ruta
Gestor de la cola de salida
Atención de cola con QoS
Atención de cola de mejor esfuerzo

Figura 19.10. Arquitectura de servicios integrados implementada en un encaminador.

Las principales funciones secundarias son las siguientes:

- **Protocolo de reserva:** este protocolo se utiliza para reservar recursos para nuevos flujos con un nivel dado de QoS. Se utiliza entre dispositivos de encaminamiento y entre encaminadores y sistemas finales. El protocolo de reserva es el responsable de mantener información de estado de cada flujo en los sistemas finales y en los dispositivos de encaminamiento que se encuentren a lo largo del camino del flujo. Para este propósito se utiliza el protocolo RSVP. El protocolo de reserva actualiza la base de datos de control de tráfico utilizada por el gestor de la cola de salida de paquetes para determinar el servicio que se le proporciona a los paquetes de cada flujo.
- **Control de admisión:** cuando se solicita un flujo nuevo, el protocolo de reserva invoca la función de control de admisión. Esta función determina si hay recursos suficientes disponibles para el flujo para esta QoS solicitada. Esta determinación se basa en el nivel actual del compromiso con otras reservas y/o la carga actual de la red.
- **Agente de gestión:** un agente de gestión de red es capaz de modificar la base de datos de control de tráfico y dirigir el módulo de control de admisión para establecer políticas de control de admisión.
- **Protocolo de encaminamiento:** el protocolo de encaminamiento es responsable de mantener la base de datos de encaminamiento que indica el siguiente salto para cada dirección destino y cada flujo.

Estas funciones de apoyo dan soporte a la tarea principal del dispositivo de encaminamiento, consistente en reenviar paquetes. Las dos áreas funcionales principales que llevan a cabo el reenvío son las siguientes:

- **Clasificación y selección de ruta:** para llevar a cabo el reenvío y el control de tráfico, los paquetes recibidos han de ser clasificados en clases. Una clase puede corresponderse con un único flujo o con un conjunto de flujos que requieran la misma QoS. Por ejemplo, los paquetes de todos los flujos de vídeo o los paquetes de todos los flujos atribuibles a una organización concreta se pueden tratar de forma idéntica a efectos de asignación de recursos y disciplinas de tratamiento de cola. La selección de clase se lleva a cabo en función de los campos de la cabecera IP. Basándose en la clase de un paquete y en su dirección IP de destino, esta función determina la dirección del siguiente salto que se debe efectuar.
- **Gestor de la cola de salida:** esta función gestiona una o más colas de cada puerto de salida. Determina el orden en el que se transmiten los paquetes de la cola de salida y selecciona los paquetes para descartarlos, si es necesario. Las decisiones se toman basándose en la clase del paquete, el contenido de la base de datos de control de tráfico y la actividad actual y pasada de este puerto de salida. Parte de la tarea del gestor de la cola de salida es la de supervisión, que es la función que determina si el tráfico de paquetes en un flujo dado excede la capacidad solicitada y, si es así, decidir cómo tratar el exceso de paquetes.

SERVICIOS ISA

El servicio ISA para un flujo de paquetes se define a dos niveles. Primero, se proporcionan varias categorías generales de servicio, cada una de las cuales proporciona cierto tipo general de garantías de servicio. En segundo lugar, dentro de cada categoría, el servicio que se le da a un flujo particular se especifica por los valores de ciertos parámetros. Juntos, a estos valores se les denomina especificación de tráfico (TSpec). Actualmente se han definido tres categorías de servicio:

- Garantizado.
- De carga controlada.
- De mejor esfuerzo.

Una aplicación puede solicitar una reserva para un flujo con QoS garantizada o de carga controlada, con una TSpec que defina la cantidad exacta del servicio solicitado. Si se acepta la reserva, entonces la TSpec forma parte del contrato entre el flujo de datos y el servicio. El servicio acepta proporcionar la QoS solicitada mientras que el tráfico del flujo de datos continúe siendo descrito de forma precisa por la TSpec. A los paquetes que no formen parte de un flujo reservado se les da por defecto un servicio del mejor esfuerzo.

Antes de examinar las categorías de servicio de ISA, se debería definir un concepto general: la especificación de tráfico por cubo de testigos. Ésta es una forma de caracterizar el tráfico que posee tres ventajas en el contexto de ISA:

1. Muchas fuentes de tráfico se pueden definir fácilmente y de forma precisa mediante un esquema de cubo de testigos.
2. El esquema de cubo de testigos proporciona una descripción concisa de la carga que va a imponer un flujo, permitiendo al servicio determinar fácilmente los recursos requeridos.
3. El esquema de cubo de testigos proporciona los parámetros de entrada a la función de supervisión.

Una especificación de tráfico por cubo de testigos consta de dos parámetros: la velocidad de entrada de testigos, R, y el tamaño del cubo, B. La tasa de entrada de testigos R especifica la velocidad de datos continua sostenible, es decir, que la tasa media de datos que se ha de admitir para un flujo durante un periodo de tiempo relativamente largo es R. El tamaño del cubo B especifica la cantidad que la velocidad de datos puede exceder de R durante periodos cortos de tiempo. La condición exacta es la siguiente: durante cualquier periodo de tiempo T, la cantidad de datos enviados no puede exceder de $RT + B$.

La Figura 19.11 ilustra este esquema y explica el uso del término *cubo*. El cubo representa un contador que indica el número permitido de octetos de datos IP que se pueden enviar en cualquier instante de tiempo. El cubo se llena con *octetos testigo* a una tasa R (en otras palabras, el contador se incrementa R veces por segundo), hasta la capacidad del cubo (hasta el valor máximo del contador). Los datagramas IP van llegando y siendo introducidos en la cola para su procesamiento. Un datagrama IP puede ser procesado si hay suficientes octetos testigo que igualen el tamaño de los datos IP. Si es así, se procesa el paquete y se consume el correspondiente número de testigos del cubo. Si llega un paquete y no hay suficientes testigos disponibles, entonces el paquete excede la TSpec de este flujo. El tratamiento que se le da a este paquete no está especificado en los documentos de ISA. Las acciones más comunes consisten en relegar el paquete a un servicio del mejor esfuerzo, descartar el paquete o marcarlo de forma que puede ser descartado en el futuro.

A la larga, la velocidad de datos IP tolerados por el cubo de testigos es R. Sin embargo, si existe un periodo de inactividad o relativamente lento, la capacidad del cubo aumenta, de forma que, como mucho, unos B octetos adicionales pueden aceptarse por encima de la tasa establecida. De esta forma, B es una medida de la longitud tolerada para las ráfagas del flujo de datos.

Servicio garantizado

Los elementos clave del servicio garantizado son los siguientes:

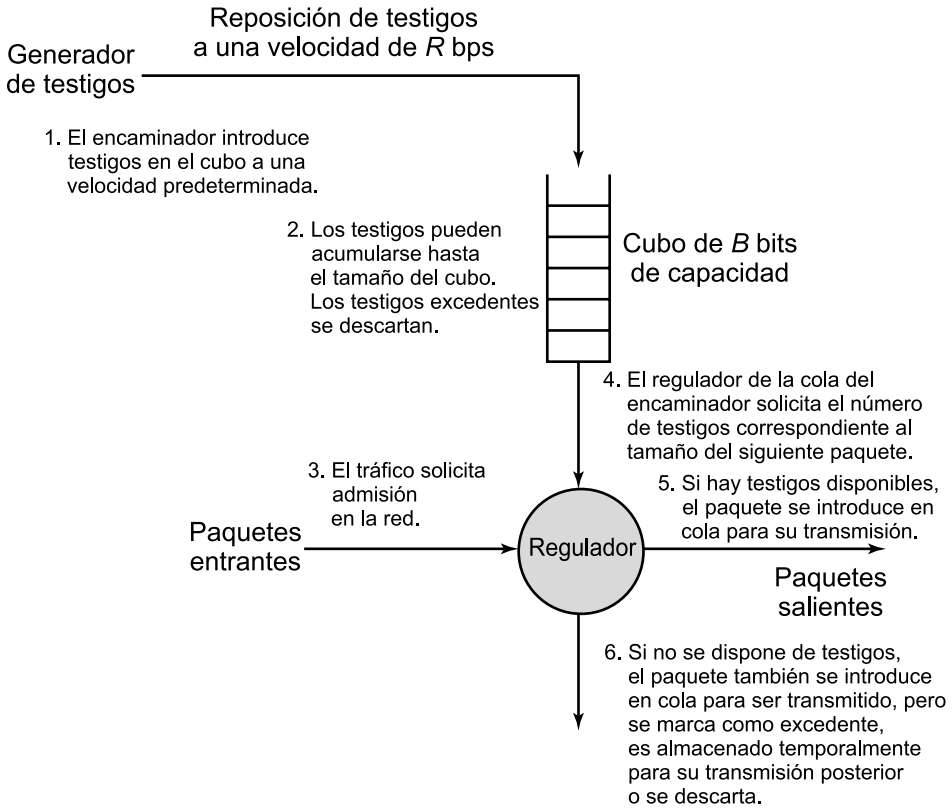


Figura 19.11. Esquema del cubo de testigos.

- El servicio proporciona una capacidad asegurada, o tasa de datos.
- Existe una especificación del límite superior para el retardo de estancia en colas a través de la red. Ésta ha de añadirse al retardo de propagación (o latencia) de llegada para obtener el límite del retardo total a través de la red.
- No se producen pérdidas en las colas. Es decir, no se pueden perder paquetes por desbordamiento de la memoria temporal. Los paquetes se pueden perder por averías en la red o por cambios en las rutas de encaminamiento.

Para este servicio, cada aplicación proporciona una caracterización de su perfil de tráfico esperado y el servicio determina el retardo extremo a extremo que puede garantizar.

Una clase de aplicaciones que utiliza este servicio lo constituyen aquellas que necesiten una cota superior de retardo, de forma que se puede utilizar una memoria temporal para reproducir en tiempo real los datos que se reciban, y que no toleren la pérdida de paquetes debido a la degradación de la calidad de la salida que se experimente. Otro ejemplo lo constituyen las aplicaciones con plazos estrictos de tiempo real.

El servicio garantizado es el servicio más exigente de los que proporciona ISA. Debido a que el límite del retardo es estricto, éste ha de establecerse a un valor alto para contemplar casos excepcionales de grandes retardos en colas.

Carga controlada

Los elementos clave del servicio de carga controlada son los siguientes:

- El servicio se ajusta al comportamiento percibido por las aplicaciones que reciben un servicio de mejor esfuerzo bajo condiciones de ausencia de carga.
- No se especifica un límite superior en el retardo de permanencia en colas a través de la red. Sin embargo, el servicio asegura que un porcentaje elevado de paquetes no experimentará retardos que excedan el retardo mínimo de tránsito (es decir, el retardo debido al tiempo de propagación más el tiempo de procesamiento en los dispositivos de encaminamiento sin el retardo de permanencia en colas).
- Un porcentaje muy alto de paquetes transmitidos son entregados correctamente (es decir, sin producirse apenas pérdidas en las colas de los encaminadores).

Como se ha mencionado anteriormente, el riesgo que se da en una interconexión de redes que proporcione QoS a aplicaciones de tiempo real es que se excluya el tráfico de mejor esfuerzo. Esto ocurre porque los tipos de aplicaciones de mejor esfuerzo utilizan TCP, que decae en presencia de congestión y retardos. El servicio de carga controlada garantiza que la red reservará suficientes recursos, de modo que una aplicación que reciba este servicio percibirá una red que responde como si esas aplicaciones en tiempo real no estuvieran presentes y compitiendo por los recursos.

El servicio controlado es útil para las aplicaciones denominadas aplicaciones en tiempo real adaptables [CLAR92]. Tales aplicaciones no requieren a priori un límite superior del retardo a través de la red. En su lugar, el receptor mide la variación del retardo experimentado por los paquetes que se reciben y ajusta el instante de reproducción al mínimo retardo que aún produzca una tasa de pérdidas suficientemente baja (por ejemplo, el vídeo puede ser adaptable descartando una trama o retrasando ligeramente el flujo de salida, la voz puede ser adaptable ajustando los periodos de silencio).

DISCIPLINAS DE ATENCIÓN DE COLA

Un componente importante de una implementación de ISA es la disciplina de atención de colas utilizada en los dispositivos de encaminamiento. Los dispositivos de encaminamiento han utilizado tradicionalmente la disciplina de atención de cola «primero en llegar primero en salir» (FIFO) en cada uno de los puertos de salida. En cada puerto de salida se mantiene una cola simple. Cuando llega un paquete y se encamina a un puerto de salida, se le sitúa al final de la cola. Mientras la cola no esté vacía, el dispositivo de encaminamiento transmite paquetes de la cola, tomando el más antiguo.

La disciplina FIFO tiene varias deficiencias:

- No se da ningún tratamiento especial a los paquetes de flujos que tengan una prioridad más alta o que sean más sensible al retardo. Si hay varios paquetes de diferentes flujos preparados para ser reenviados, todos ellos se procesan en un estricto orden FIFO.
- Si varios paquetes pequeños se sitúan en cola detrás de un paquete de gran tamaño, entonces la disciplina FIFO da lugar a un retardo medio por paquete mayor que si los paquetes pequeños se transmitieran antes que el grande. En general, los flujos con paquetes grandes obtienen un mejor servicio.

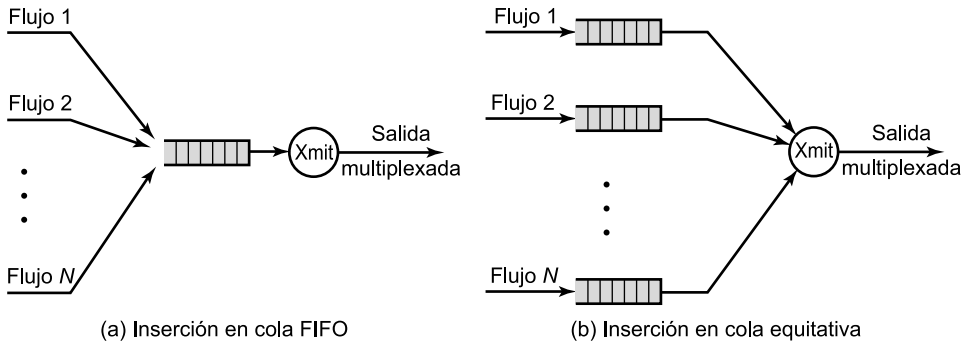


Figura 19.12. Inserciones en cola FIFO y equitativas.

- Una conexión TCP codiciosa puede excluir a otras conexiones altruistas. Si aparece la congestión y una conexión no decae, otras conexiones que utilicen el mismo segmento de la ruta deben decaer más de lo que deberían en otras circunstancias.

Para resolver las deficiencias de la disciplina FIFO, se utiliza un tipo de esquema de atención equitativo de la cola, en el que un dispositivo de encaminamiento mantiene múltiples colas para cada puerto de salida (*véase* Figura 19.12). Con una atención equitativa simple de la cola, cada paquete de entrada se sitúa en una cola para su correspondiente flujo. Las colas se atienden de forma cíclica, tomando un paquete de cada cola no vacía por turno. Las colas vacías no se atienden. Este esquema es equitativo en el sentido de que cada flujo consigue enviar exactamente un paquete por ciclo. Además, constituye también una forma de balancear la carga entre varios flujos. No hay ninguna ventaja para las conexiones codiciosas. Un flujo codicioso observa que su cola se va llenando, incrementando su retardo, mientras que los otros flujos no se ven afectados por este comportamiento.

Algunos fabricantes han implementado una mejora de la atención equitativa de colas conocido como atención de colas equitativa ponderada (WFQ, *Weighted Fair Queuing*). De forma resumida, WFQ tiene en cuenta la cantidad de tráfico de cada cola y asigna más capacidad a las colas más ocupadas sin dejar de atender a las colas menos ocupadas. Además, WFQ puede tener en cuenta la cantidad de servicio solicitado por el tráfico de cada flujo y ajustar la disciplina de atención de cola de acuerdo al mismo.

PROTOCOLO DE RESERVA DE RECURSOS

El RFC 2205 define el protocolo de reserva de recursos (RSVP, *Resource ReSerVation Protocol*), el cual proporciona funcionalidad de apoyo a ISA. Esta subsección proporciona una visión general de RSVP.

Una tarea clave, tal vez la tarea crucial en una interconexión de redes, es la distribución de datos desde una fuente a uno o más destinos con la calidad del servicio (QoS) solicitada, como puede ser el rendimiento, retardo, variación del retardo, etcétera. Esta tarea crece en dificultad en cualquier interconexión de redes cuando se incrementa el número de usuarios o la velocidad de transmisión de las aplicaciones y con el empleo de la multidifusión. Para satisfacer estas necesidades, para la red no es suficiente con reaccionar ante la congestión. En su lugar, es necesaria una herramienta que prevenga la congestión permitiendo a las aplicaciones reservar recursos de red para una QoS dada.

Las medidas preventivas pueden ser útiles en ambos tipos de transmisión (monodifusión y multidifusión). Para la **monodifusión**, dos aplicaciones acuerdan una calidad de servicio específica para una sesión y esperan que la interconexión de redes proporcione esa calidad de servicio. Si la red está muy cargada, puede que no proporcione la QoS deseada y, en su lugar, se distribuyan los paquetes con una QoS inferior. En este caso, las aplicaciones podrían preferir esperar antes de iniciar la sesión, o al menos ser alertadas de la posibilidad de obtener una QoS inferior. Una forma de tratar esta situación consiste en que las aplicaciones de monodifusión reserven recursos para garantizarse una calidad de servicio determinada. Los dispositivos de encaminamiento a lo largo del camino previsto pueden entonces preasignar recursos (espacio en las colas y capacidad de salida) para asegurar la QoS deseada. Si un encaminador no pudiera satisfacer la reserva de recursos debido a reservas vigentes asignadas con anterioridad, entonces se podría informar a las aplicaciones de este hecho. Así, las aplicaciones podrían elegir entre intentar de nuevo la reserva con una QoS inferior o intentarlo más tarde.

La transmisión en **multidifusión** presenta un caso mucho más apremiante para la implementación de la reserva de recursos. Una transmisión en multidifusión puede generar una cantidad enorme de tráfico de red si la aplicación genera gran volumen de datos (por ejemplo, vídeo) o el grupo de multidifusión destino es grande y disperso, o ambas cosas a la vez. Lo que justifica la reserva de recursos para la multidifusión es que mucha de la carga potencial generada por una fuente de multidifusión se puede evitar fácilmente. Esto es así por dos razones:

1. Algunos de los miembros de un grupo multidifusión existente pueden no necesitar la distribución desde una fuente determinada durante un periodo de tiempo dado. Por ejemplo, puede haber dos «canales» (dos fuentes de multidifusión) transmitiendo a un grupo de multidifusión particular al mismo tiempo. Un destino de multidifusión podría querer «sintonizar» sólo uno de los canales en un momento dado.

2. Algunos miembros de un grupo podrían ser capaces de procesar sólo una parte de la transmisión de la fuente. Por ejemplo, una fuente de vídeo puede transmitir un flujo de vídeo que conste de dos componentes: una componente básica que proporcione una reducida calidad de imagen y una componente de realce. Puede que algunos receptores no tengan la potencia de procesamiento suficiente para procesar la componente de realce, o pueden estar conectados a la interconexión de redes a través de una subred o enlace que no tenga suficiente capacidad para la señal completa.

En consecuencia, la utilización de la reserva de recursos puede permitir a los dispositivos de encaminamiento decidir con antelación si pueden satisfacer las necesidades de la distribución de una transmisión en multidifusión a todos los destinos de la multidifusión indicados y reservar, si fuera posible, los recursos apropiados.

La reserva de recursos en una interconexión de redes se diferencia del tipo de reserva de recursos que se puede implementar en una red orientada a conexión, como es ATM o retransmisión de tramas. Un esquema de reserva de recursos en una interconexión de redes debe interaccionar con una estrategia de encaminamiento dinámica que permita cambiar la ruta seguida por los paquetes de una transmisión dada. Cuando la ruta cambia, las reservas de recursos deben cambiar. Para tratar esta situación dinámica se utiliza el concepto de **estado temporal** (*soft state*). Un estado temporal es simplemente un conjunto de información de estado en un dispositivo de encaminamiento que expira a menos que la entidad que solicita el estado la actualice regularmente. Si la ruta de una transmisión dada cambia, algunos estados temporales expirarán y una nueva reserva de recursos establecerá los estados temporales correspondientes en los encaminadores a lo largo de la nueva

ruta. De este modo, los sistemas finales que solicitan los recursos deben renovar periódicamente sus solicitudes durante el curso de la transmisión de la aplicación.

Basándose en las anteriores consideraciones, la especificación describe las siguientes características de RSVP:

- **Monodifusión y multidifusión:** RSVP admite reservas para ambos tipos de transmisión, adaptándose dinámicamente a los cambios de pertenencias a grupos, así como a los cambios de rutas, y reservando recursos basándose en las necesidades individuales de los miembros del grupo de multidifusión.
- **Simplex:** RSVP establece reservas para flujos de datos en un solo sentido. El intercambio de datos entre dos sistemas finales requiere reservas separadas en los dos sentidos.
- **Reserva iniciada por el receptor:** el receptor de un flujo de datos inicia y mantiene la reserva de recursos para ese flujo.
- **Mantenimiento del estado temporal en la interconexión de redes:** RSVP mantiene un estado temporal en los dispositivos de encaminamiento intermedios y delega en los usuarios finales la responsabilidad de mantener activos estos estados de reserva.
- **Proporciona diferentes estilos de reservas:** estos estilos permiten a los usuarios de RSVP especificar cómo se deberían agregar en los conmutadores intermedios las reservas para el mismo grupo de multidifusión. Esta característica permite un uso más eficiente de los recursos de la red.
- **Funcionamiento transparente a través de dispositivos de encaminamiento no RSVP:** ya que las reservas y RSVP son independientes del protocolo de encaminamiento, no existen conflictos graves en un entorno mixto en el que algunos dispositivos de encaminamiento no utilicen RSVP. Estos encaminadores simplemente utilizarán la técnica de transporte de mejor esfuerzo.
- **Soporte para IPv4 e IPv6:** RSVP puede hacer uso del campo «tipo de servicio» de la cabecera de IPv4 y del campo «etiqueta de flujo» de la cabecera de IPv6.

19.4. SERVICIOS DIFERENCIADOS

La arquitectura de servicios integrados (ISA) y RSVP están pensados para permitir ofrecer calidad de servicio (QoS) en Internet y en redes privadas. Aunque ISA en general, y RSVP en particular, son herramientas útiles para este propósito, dichas características son relativamente complejas de implementar. Además, pueden no ser lo suficientemente escalables como para tratar grandes volúmenes de tráfico, debido a la cantidad de señalización de control necesaria para coordinar la oferta de QoS integrada y al mantenimiento de la información de estado necesaria en los dispositivos de encaminamiento.

A medida que la carga en Internet aumenta, así como la diversidad de aplicaciones, existe una necesidad inmediata de proporcionar niveles diferenciados de QoS a diferentes flujos de tráfico. La arquitectura de servicios diferenciados (DS, *Differentiated Services*, *RFC 2475*) está diseñada para proporcionar una herramienta simple, fácil de implementar y que suponga una escasa sobrecarga que ofrezca distintos servicios de red que estén diferenciados según su rendimiento.

Varias características clave de DS contribuyen a su eficiencia y facilitan su implementación:

- Los paquetes se etiquetan para un tratamiento de QoS diferenciado utilizando el octeto de tipo de servicio de IPv4 (*véase* Figura 18.6) o el octeto de clase de tráfico de IPv6 (*véase* Figura 18.11). Por lo tanto, no se necesita efectuar cambios en IP.
- Antes de utilizar DS se establece un acuerdo de nivel de servicio (SLA, *Service Level Agreement*) entre el proveedor de servicios (dominio de red) y el cliente. Esto evita la necesidad de incorporar los mecanismos de DS en las aplicaciones. Así, no se necesita modificar las aplicaciones existentes para utilizar DS.
- Los DS proporcionan un mecanismo de agregación integrado. Todo el tráfico con el mismo octeto DS es tratado de igual forma por el servicio de red. Por ejemplo, múltiples conexiones de voz no se tratan de forma individual sino en conjunto. Esto permite que sea escalable para redes extensas y elevadas cargas de tráfico.
- Los DS se implementan en dispositivos de encaminamiento individuales mediante la atención en cola y el reenvío de paquetes basándose en el octeto DS. Los encaminadores tratan cada paquete individualmente y no tienen que guardar información de estado sobre flujos de paquetes.

Hoy en día, DS es el mecanismo de provisión de QoS más extendido en redes empresariales. Aunque DS pretende proporcionar un servicio simple basándose en mecanismos relativamente sencillos, el conjunto de RFC relacionados con DS es relativamente complejo. La Tabla 19.4 resume algunos de los términos clave obtenidos de esas especificaciones.

SERVICIOS

El tipo de servicio de DS se proporciona dentro de un dominio DS, que se define como una porción contigua de Internet sobre la que se administra un conjunto consistente de políticas de DS. Normalmente, un dominio de DS debería estar bajo el control de una única entidad administrativa. Los servicios proporcionados a través de un dominio DS se definen en un acuerdo de nivel de servicio (SLA), que es un contrato de servicio entre el cliente y el proveedor de servicios donde se especifica el servicio de reenvío que recibirá el cliente para varias clases de paquetes. Un cliente podría ser una organización u otro dominio de DS. Una vez que se establece el SLA, el cliente emite paquetes con el octeto DS marcado para indicar la clase del paquete. El proveedor de servicios debe asegurar que el cliente obtiene al menos la QoS acordada para cada clase de paquete. Para proporcionar esa QoS, el proveedor de servicios debe configurar las políticas de reenvío apropiadas en cada dispositivo de encaminamiento (basándose en el valor del octeto DS) y debe monitorizar el rendimiento que se está proporcionando a cada clase basándose en el comportamiento en curso.

Si un cliente envía un paquete dirigido a destinos dentro del mismo dominio de DS, entonces se espera que el dominio DS proporcione el servicio acordado. Si el destino está más allá del dominio de DS del cliente, entonces el dominio de DS intentará reenviar los paquetes a través de otros, solicitando el servicio más apropiado para ajustarse al servicio solicitado.

Un borrador del documento de trabajo sobre DS indica los siguientes parámetros detallados de funcionamiento que podrían incluirse en una SLA:

- Parámetros detallados de las prestaciones del servicio, como rendimiento esperado, probabilidad de descarte y latencia.
- Restricciones en los puntos de entrada y salida a través de los que se suministra el servicio, indicando el ámbito del mismo.

Tabla 19.4. Terminología de los servicios diferenciados.

Agregado de comportamiento	Conjunto de paquetes con el mismo código DS que cruza un enlace en un sentido concreto.
Clasificador	Selecciona paquetes basándose en el campo DS (clasificador BA) o en varios campos de la cabecera del paquete (clasificador MF).
Nodo DS frontera	Nodo DS que conecta un dominio de DS con otro nodo en otro dominio.
Código DS	Valor específico de la sección DSCP (6 bits) del campo DS (8 bits) en la cabecera IP.
Dominio de DS	Conjunto de nodos contiguos (conectados), capaces de implementar servicios diferenciados, que operan con un conjunto común de políticas de suministro de servicios y definiciones de comportamiento en cada salto.
Nodo DS interior	Nodo DS que no es un nodo frontera.
Nodo DS	Nodo que proporciona servicios diferenciados. Normalmente, un nodo DS es un dispositivo de encaminamiento. Un computador que proporcione servicios diferenciados para las aplicaciones que ejecuta también es un nodo DS.
Descarte	Proceso de descarte de paquetes basándose en reglas específicas. También se le llama supervisión.
Marcado	Proceso de asignación del código DS en un paquete. Los paquetes se pueden marcar en el inicio y pueden ser remarcados por un nodo DS en la ruta.
Monitorización	Proceso de medir las propiedades temporales (por ejemplo, la tasa) de un flujo de paquetes seleccionado por un clasificador. El estado instantáneo de ese proceso puede influir en las funciones de marcado, conformado y descarte.
Comportamiento por salto (PHB)	Comportamiento de reenvío observable externamente aplicado en un nodo a un agregado de comportamiento.
Acuerdo de nivel de servicio (SLA)	Contrato de servicio entre un cliente y un proveedor de servicios, donde se especifica el servicio de reenvío que debe recibir un cliente.
Conformado	Proceso de retrasar paquetes en un flujo de paquetes para ajustarlo a algún perfil de tráfico definido.
Acondicionamiento de tráfico	Funciones de control que se llevan a cabo para hacer cumplir las reglas especificadas en un TCA, incluyendo monitorización, marcado, conformado y descarte.
Acuerdo de acondicionamiento de tráfico (TCA)	Acuerdo que especifica reglas de clasificación y reglas de acondicionamiento de tráfico que se han de aplicar a los paquetes seleccionados por el clasificador.

- Perfiles de tráfico a los que se debe ajustar para recibir el servicio solicitado, como por ejemplo los parámetros del cubo de testigos.
- Disposición del tráfico generado que exceda el perfil especificado.

Este documento de trabajo proporciona también algunos ejemplos de servicios que se podrían suministrar:

1. El tráfico ofrecido en el nivel de servicio A será entregado con una baja latencia.
2. El tráfico ofrecido en el nivel de servicio B será entregado con una baja tasa de pérdidas.

3. El noventa por ciento del perfil de tráfico entregado con el nivel de servicio C no experimentará más de 50 ms de latencia.
4. El noventa y cinco por ciento del perfil de tráfico distribuido con el nivel de servicio D será entregado.
5. El tráfico ofrecido en el nivel de servicio E tendrá asignado el doble de ancho de banda que el tráfico ofrecido en el nivel de servicio F.
6. El tráfico con precedencia de descarte X tiene una probabilidad mayor de entrega que el tráfico con precedencia de descarte Y.

Los primeros dos ejemplos son cualitativos y son sólo válidos en comparación con otro tipo de tráfico, como el tráfico por defecto que obtiene un servicio de mejor esfuerzo. Los dos ejemplos siguientes son cuantitativos y proporcionan una garantía específica que puede ser verificada mediante la medida del servicio real, sin necesidad de comparar con otros servicios ofrecidos al mismo tiempo. Los dos ejemplos finales son una mezcla de ejemplos cualitativos y cuantitativos.

OCTETO DS

Los paquetes se etiquetan para el tratamiento del servicio por medio del octeto DS, el cual se sitúa en el campo tipo de servicio de la cabecera de IPv4, o en el campo clase de tráfico de la cabecera IPv6. El RFC 2474 define el octeto DS con el siguiente formato: los 6 bits más a la izquierda forman el código DS y los dos bits más a la derecha no se utilizan. El código de DS es la etiqueta de DS utilizada para clasificar los paquetes para los servicios diferenciados. La Figura 19.13a muestra este campo DS.

Con un código de 6 bits, se pueden definir en principio 64 clases de tráfico diferentes. Estos 64 códigos se agrupan en tres conjuntos de códigos, como se indica a continuación:

- Los códigos de la forma xxxxx0, donde x es 0 o 1, están reservados para su asignación como estándares.
- Los códigos de la forma xxxx11 están reservados para uso experimental o local.
- Los códigos de la forma xxxx01 están también reservados para un uso experimental o local, pero se pueden asignar para estándares futuros según se necesite.

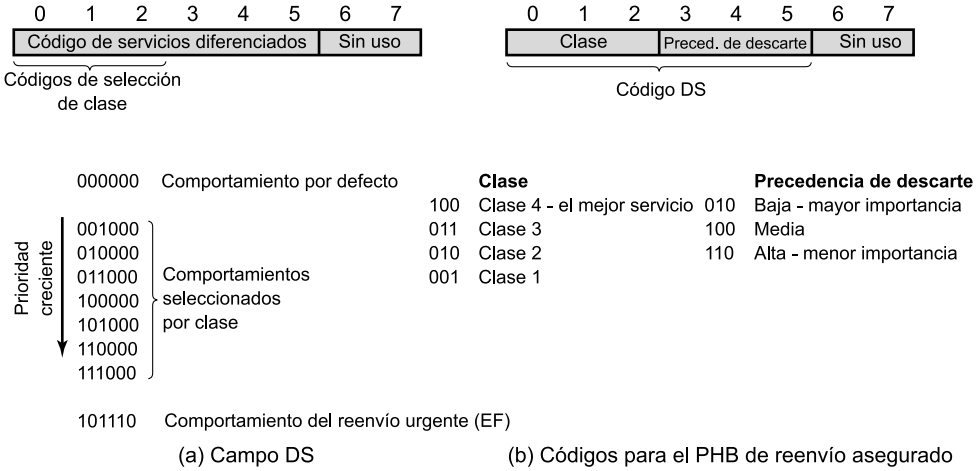


Figura 19.13. Campo DS.

En el RFC 2474 se establecen varias asignaciones dentro del primer grupo. El código 000000 es la clase de paquete por defecto. La clase por defecto corresponde al comportamiento de reenvío de mejor esfuerzo de los dispositivos de encaminamiento existentes. Tales paquetes se reenvían en el orden en el que son recibidos tan pronto como la capacidad del enlace esté disponible. En caso de que haya paquetes de otras clases de DS con mayor prioridad, se les da preferencia sobre los paquetes de mejor esfuerzo.

Los códigos de la forma xxx000 están reservados para proporcionar compatibilidad hacia atrás con el servicio de precedencia de IPv4. Para explicar este requisito, necesitamos realizar un inciso para explicar el servicio de precedencia de IPv4. El campo de tipo de servicio (TOS) de IPv4 incluye dos subcampos: un campo de precedencia de 3 bits y un subcampo de TOS de 4 bits. Estos subcampos atienden funciones complementarias. El subcampo de TOS proporciona orientación a la entidad IP (en la fuente o en el dispositivo de encaminamiento) para seleccionar el siguiente salto para este datagrama y el subcampo de precedencia orienta acerca de la asignación relativa de los recursos del encaminador para el datagrama.

El campo de precedencia se establece para indicar el grado de urgencia o prioridad que se le va a asociar a un datagrama. Si el dispositivo de encaminamiento reconoce el subcampo de precedencia, existen tres reacciones posibles:

- **Selección de ruta:** se puede seleccionar una ruta particular si el encaminador tiene una cola menos ocupada para esa ruta o si el siguiente salto en esa ruta permite la precedencia o prioridad de red (por ejemplo, una red de paso de testigo permite prioridad).
- **Servicio de red:** si la red en el siguiente salto tiene soporte para la precedencia se invoca ese servicio.
- **Disciplina de atención de cola:** un dispositivo de encaminamiento puede utilizar precedencia para influir en cómo se procesan las colas. Por ejemplo, un dispositivo de encaminamiento puede dar un tratamiento preferencial en las colas a datagramas con una precedencia más alta.

En el RFC 1812, «Requisitos para los dispositivos de encaminamiento con IP versión 4», se proporcionan recomendaciones para la disciplina de atención de colas, englobadas en dos categorías:

- **Servicio de atención de cola**

  a) Los dispositivos de encaminamiento DEBEN implementar un servicio de cola ordenado por precedencia. Un servicio de cola ordenado por precedencia implica que, cuando se selecciona un paquete para su emisión por un enlace (lógico), se envía el paquete con la precedencia más alta que haya sido situado en cola para ese enlace.

  b) Cualquier dispositivo de encaminamiento PUEDE implementar otras políticas basadas en procedimientos de gestión del rendimiento que sean distintas a la estricta ordenación por precedencia, pero DEBE ser configurable para deshabilitarlas (es decir, poder utilizar orden estricto).

- **Control de congestión.** Cuando un dispositivo de encaminamiento supera su capacidad de almacenamiento y recibe un nuevo paquete, debe descartar este último o alguno o varios de los otros paquetes.

  a) Un dispositivo de encaminamiento PUEDE descartar el paquete que acaba de recibir. Ésta es la política más simple, pero no la mejor.

b) Idealmente, el dispositivo de encaminamiento debe seleccionar el paquete de una de las sesiones que mayor abuso hagan del enlace, suponiendo que la política aplicable de QoS permita esto. Una política recomendable en un entorno de datagramas que utilice colas FIFO consiste en descartar un paquete de la cola seleccionado de forma aleatoria. Un algoritmo equivalente en encaminadores que utilicen colas equitativas consiste en descartar de la cola más larga. Un dispositivo de encaminamiento PUEDE utilizar estos algoritmos para determinar qué paquete descartar.

c) Si se implementa un servicio de cola con ordenación de precedencia y está activado, el dispositivo de encaminamiento NO DEBE descartar un paquete cuya precedencia de IP sea más alta que la de un paquete que no se descarte.

d) Un dispositivo de encaminamiento PUEDE proteger paquetes cuya cabecera IP solicite la máxima fiabilidad de TOS, excepto en el caso en que suponga violar la regla anterior.

e) Un dispositivo de encaminamiento PUEDE proteger paquetes IP fragmentados, justificado por el hecho de que descartar un fragmento de un datagrama puede incrementar la congestión causando que la fuente deba retransmitir todos los fragmentos del paquete.

f) Para evitar las perturbaciones en el encaminamiento o la interrupción de las funciones de gestión, el dispositivo de encaminamiento PUEDE proteger los paquetes utilizados para el control del encaminamiento, el control de enlace o la gestión de red, para que no sean descartados. Los encaminadores dedicados (es decir, los dispositivos de encaminamiento que no sean además computadores de propósito general, servidores de terminales, etc.) pueden lograr una aproximación a esta regla protegiendo los paquetes cuya fuente o destino sea el propio dispositivo de encaminamiento.

Los códigos de DS de la forma xxx000 deben proporcionar un servicio que, como mínimo, sea equivalente a la funcionalidad de precedencia de IPv4.

CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS DS

La Figura 19.14 muestra el tipo de configuración prevista en los documentos sobre los DS. Un dominio de DS consta de un conjunto de dispositivos de encaminamiento contiguos. Esto significa que es posible llegar desde cualquier dispositivo de encaminamiento en el dominio a cualquier otro encaminador en el mismo dominio, a través de un camino que no incluya dispositivos de encaminamiento externos al dominio. Dentro de un dominio, la interpretación de los códigos de DS es uniforme, de forma que se proporciona un servicio uniforme y consistente.

Los encaminadores de un dominio de DS pueden ser nodos frontera o nodos interiores. Normalmente, los nodos interiores implementan mecanismos simples para procesar los paquetes basándose en los valores de su código de DS. Esto incluye la disciplina de atención de cola para dar un tratamiento preferencial basado en el valor del código y las reglas de descarte de paquetes que dictan qué paquetes se deberían descartar primero en caso de que se sature la memoria temporal. Las especificaciones de DS denominan comportamiento por salto (PHB, *Per-Hop Behavior*) del encaminador al tratamiento de reenvío que se proporciona en el mismo. Este PHB debe estar disponible en todos los dispositivos de encaminamiento y, normalmente, el PHB es la única parte de DS implementada en los dispositivos de encaminamiento interiores.

Los nodos frontera incluyen mecanismos de PHB, pero necesitan además mecanismos de acondicionamiento del tráfico más sofisticados para proporcionar el servicio deseado. Así, los dispositivos de encaminamiento interiores tienen una funcionalidad y sobrecarga mínimas al proporcionar

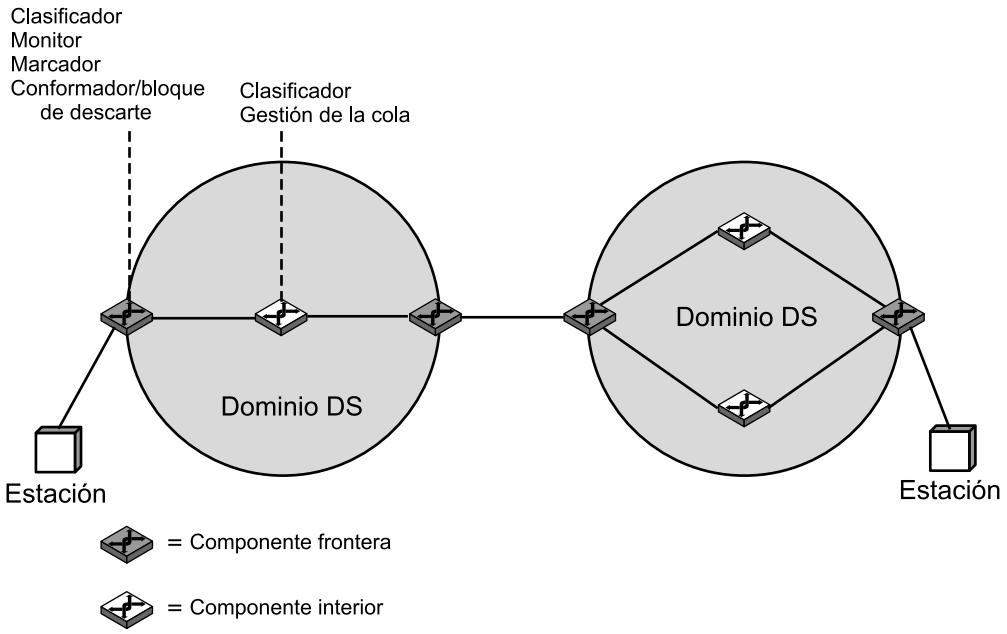


Figura 29.4. Dominios DS.

el servicio de DS, mientras que la mayor parte de la complejidad se sitúa en los nodos frontera. La función de un nodo frontera también la puede suministrar una estación de ese dominio, en nombre de las aplicaciones de ese computador.

La función de acondicionamiento del tráfico consta de cinco elementos:

- **Clasificador:** separa en clases diferentes los paquetes enviados. Ésta es la base de la provisión de servicios diferenciados. Un clasificador puede separar el tráfico basándose sólo en el código de DS (clasificador de comportamiento agregado), basándose en múltiples campos de la cabecera del paquete o, incluso, de los datos del paquete (clasificador multicampo).
- **Monitor:** mide el tráfico enviado para comprobar que se ajusta a un perfil. El medidor determina si una clase de flujo de paquetes dada cumple o excede el nivel de servicio garantizado para esa clase.
- **Marcador:** remarca los paquetes con un código diferente según se necesite. Esto se puede hacer para paquetes que excedan el perfil. Por ejemplo, si se garantiza un rendimiento dado para una clase de servicio determinado, cualquier paquete de esa clase que exceda la tasa en algún intervalo de tiempo definido se puede remarcar para tratarse con el servicio de mejor esfuerzo. También se puede necesitar el remarcado en la frontera entre dos dominios de DS. Por ejemplo, si una clase de tráfico dada va a recibir la prioridad más alta, y ésta tiene el valor 3 en un dominio y 7 en el dominio siguiente, entonces los paquetes con una prioridad 3 que transiten por el primer dominio se remarcan con prioridad 7 cuando entran en el segundo dominio.
- **Conformador:** retarda los paquetes tanto como sea necesario para que el flujo de paquetes de una clase dada no exceda la tasa de tráfico especificada en su perfil.
- **Bloque de descarte de paquetes:** descarta paquetes cuando la tasa de paquetes de una clase dada excede la tasa especificada en el perfil de esa clase.

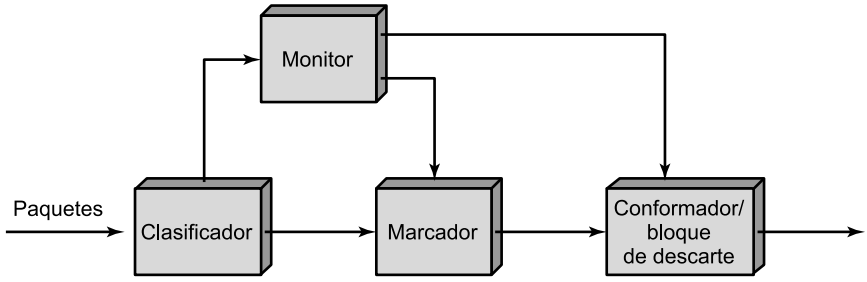


Figura 19.15. Acondicionador de tráfico DS.

La Figura 19.15 muestra la relación entre los elementos de acondicionamiento del tráfico. Después de clasificar un flujo, se debe medir su consumo de recursos. La función de monitorización mide el volumen de paquetes en un intervalo de tiempo dado para determinar si el flujo cumple el contrato de tráfico. Si el computador tiene un comportamiento de transmisión a ráfagas, para capturar las características de tráfico deseadas puede que no sea suficiente utilizar simplemente la tasa de datos o la tasa de paquetes. El esquema del cubo de testigos, como el que se muestra en la Figura 19.11, es un ejemplo de cómo definir un perfil de tráfico para tener en cuenta tanto la tasa de paquetes como el comportamiento de transmisión a ráfagas.

Se pueden seguir varias alternativas si un flujo de tráfico excede algún perfil. Los paquetes individuales que excedan el perfil pueden ser remarcados para un tratamiento con una calidad inferior y permitirles pasar al dominio de DS. Un conformador de tráfico puede absorber una ráfaga de paquetes en una memoria temporal y liberar los paquetes durante un mayor periodo de tiempo. Un bloque de descarte de paquetes puede descartar paquetes si dicha memoria temporal se satura.

COMPORTAMIENTO POR SALTO

Como parte del intento de estandarización de los DS, es necesario definir tipos específicos de PHB, que pueden ser asociados a servicios diferenciados específicos. Actualmente, dos PHB estándares han sido publicados: PHB de reenvío urgente (RFC 3246) y PHB de reenvío asegurado (RFC 2597).

PHB de reenvío urgente

El RFC 3246 define el PHB de reenvío urgente (EF, *Expedited Forwarding*) como un mecanismo que puede utilizarse para proporcionar un servicio de calidad superior. Un servicio de calidad superior es un servicio extremo a extremo con una baja tasa de pérdidas, bajo retardo, con baja fluctuación del retardo y ancho de banda asegurado, a través de dominios de DS. En esencia, los extremos perciben el servicio de calidad suprema como una conexión punto a punto o como una línea privada.

En una red de conmutación de paquetes o una interconexión de redes, es difícil conseguir un servicio de calidad superior. Por su naturaleza, una interconexión de redes implica colas en cada nodo o encaminador, donde los paquetes son almacenados temporalmente esperando utilizar un enlace de salida compartido. Es el comportamiento de la espera en cola en cada nodo lo que origina las pérdidas, los retardos y la variación en los retardos. Así, a menos que se sobredimensione en exceso la red, para eliminar todos los efectos de estancia en cola se debe tener cuidado a la hora de

procesar tráfico al que se le ha concedido el servicio de calidad superior, para asegurar que la espera en cola no produzca pérdidas, retardo o fluctuación en los retardos por encima de un umbral dado. El RFC 3246 apunta que un servicio de calidad superior tiene dos partes:

- Configuración de los nodos de forma que la agregación de tráfico[4] tenga una tasa de salidas mínima bien definida, donde aquí *bien definido* significa «independiente del estado dinámico del nodo». En particular, independiente de la intensidad de otro tráfico en el nodo.
- Acondicionamiento de la agregación (vía supervisión y conformado) de forma que su tasa de llegada a cualquier nodo sea siempre menor que la mínima tasa de salida configurada para ese nodo.

El PHB EF proporciona la primera de las dos funcionalidades indicadas, mientras que la segunda funcionalidad la proporcionan los acondicionadores de las fronteras de la red. El concepto general esbozado en el RFC 3246 es el siguiente: los nodos frontera controlan la agregación de tráfico para limitar sus características (tasa y transmisión a ráfagas) a un nivel predefinido. Los nodos interiores deben tratar el tráfico que se recibe de forma que no aparezcan los efectos de espera en cola. En términos generales, se requiere en los nodos interiores que la tasa máxima de llegada de tráfico agregado debe ser menor que la tasa mínima de salida.

El RFC 3246 no impone una política específica de atención de cola en los nodos interiores para implementar el PHB de EF. El RFC comenta que un esquema simple de prioridad podría lograr el efecto deseado, dando al tráfico EF prioridad absoluta sobre otro tráfico. Mientras el tráfico de EF no sobrecargue un nodo interior, este esquema obtendrá retardos de estancia en cola aceptables para el PHB de EF. Sin embargo, el riesgo de utilizar un esquema de prioridad simple consiste en que el flujo de paquetes del tráfico de otro PHB podría ser interrumpido. Así, podría preferirse alguna política de atención de cola más sofisticada.

PHB de reenvío asegurado

El PHB de reenvío asegurado (AF, *Assured Forwarding*) fue concebido para proporcionar un servicio superior al de mejor esfuerzo, que no requiriera la reserva de recursos dentro de la red ni una discriminación detallada entre flujos de diferentes usuarios. El concepto subyacente del PHB de AF fue presentado en [CLAR98], referido como reserva explícita. El PHB de AF es más complejo, pero será útil destacar primero los elementos clave del esquema de reserva explícita:

1. A los usuarios se les ofrece la elección de varias clases de servicio para su tráfico. Cada clase describe un perfil de tráfico diferente en términos de una tasa de datos y comportamiento de ráfagas agregados.
2. El tráfico de una clase dada de un usuario se monitoriza en un nodo frontera. Cada paquete de un flujo de tráfico se marca como *cumplidor* o *no cumplidor* basándose en si excede o no el perfil de tráfico.
3. Dentro de la red, no hay separación entre el tráfico de diferentes usuarios o incluso tráfico con diferentes clases. En su lugar, todo el tráfico se trata como un solo conjunto de paquetes, con la única distinción de si ha sido marcado como *cumplidor* o *no cumplidor*.
4. Cuando se presenta la congestión, los nodos interiores implementan un esquema de descarte en el que los paquetes *no cumplidores* son descartados antes que los paquetes *cumplidores*.

[4] El término *agregación de tráfico* se refiere al flujo de paquetes asociados con un servicio en particular para un usuario en particular.

5. Usuarios diferentes percibirán diferentes niveles de servicio porque tendrán diferente cantidad de paquetes *cumplidores* en las colas de servicio.

La ventaja de este enfoque es su simplicidad. Los nodos internos realizan muy poco trabajo. El etiquetado del tráfico basado en los perfiles de tráfico en los nodos frontera proporciona diferentes niveles de servicio a las distintas clases.

El PHB de AF definido en el RFC 2597 extiende la anterior aproximación mediante las siguientes medidas:

1. Se definen cuatro clases de AF, permitiendo la definición de cuatro perfiles de tráfico distintos. Un usuario puede seleccionar una o más de esas clases para satisfacer sus necesidades.
2. Dentro de cada clase, los paquetes son etiquetados por el cliente o por el proveedor del servicio con uno de tres valores de precedencia de descarte. En caso de congestión, la precedencia de descarte del paquete determina su importancia relativa dentro de la clase de AF. Un nodo DS congestionado intenta proteger los paquetes con menor valor de precedencia de descarte para que no sean perdidos, descartando preferentemente paquetes con un valor de precedencia de descarte mayor.

Esta aproximación es todavía más simple de implementar que cualquier tipo de esquema de reserva de recursos, pero proporciona una flexibilidad considerable. En un nodo de DS interior, el tráfico de las cuatro clases puede tratarse por separado, con diferente cantidad de recursos (espacio de memoria temporal y tasa de datos) asignados a las cuatro clases. Para cada clase, los paquetes se atienden según su precedencia de descarte. Así, como se apunta en el RFC 2597, el nivel de seguridad de reenvío de un paquete IP depende de:

- Cuántos recursos de reenvío han sido asignados a la clase AF a la que pertenece el paquete.
- La actual carga de la clase AF.
- En caso de congestión, dentro de la clase AF, la precedencia de descarte del paquete.

El RFC 2597 no establece ningún mecanismo para gestionar el tráfico AF en los nodos interiores. En él se referencia al algoritmo RED como posible alternativa para la gestión de la congestión.

En la Figura 19.13b se muestran los códigos para el PHB de AF recomendados para el campo DS.

19.5. LECTURAS Y SITIOS WEB RECOMENDADOS

[HUIT00], [BLAC00] y [PERL00] ofrecen una valiosa descripción en detalle de diversos algoritmos de encaminamiento. En [MOY98] se realiza un profundo estudio sobre OSPF.

Posiblemente, el libro más claro y exhaustivo sobre QoS en Internet es [ARMI00]. [XIAO99] ofrece una descripción y un marco generales sobre la QoS en Internet, así como de los servicios integrados y diferenciados. [CLAR92] y [CLAR95] proporcionan valiosos estudios sobre las cuestiones implicadas en la reserva de servicios en redes interconectadas para aplicaciones en tiempo real y elásticas, respectivamente. [SHEN95] presenta un análisis magistral de los fundamentos para una arquitectura de red basada en QoS. [ZHAN95] realiza un amplio estudio de las disciplinas de atención de cola que se pueden utilizar en una ISA, incluyendo un análisis de FQ y WFQ.

[ZHAN93] presenta una buena descripción general de la filosofía y funcionalidad de RSVP, escrita por sus desarrolladores. [WHIT97] contiene un estudio general de ISA y RSVP.

[CARP02] y [WEIS98] constituyen dos instructivos estudios sobre los servicios diferenciados, mientras que [KUMA98] examina los servicios diferenciados y los mecanismos de soporte de los dispositivos de encaminamiento que van más allá de los actuales RFC. Para un profundo tratamiento sobre los DS, consultar [KILK99].

Por último, los artículos [BERN00] y [HARJ00] realizan una comparación entre los IS y los DS en términos de servicios y rendimiento.

ARMI00 Armitage, G. *Quality if Service in IP Networks*. Indianapolis, IN: Macmillan Technical Publishing, 2000.

BERN00 Bernet, Y. «The Complementary Roles of RSVP and Differentiated Services in the Full-Service QoS Network». *IEEE Communications Magazine*, febrero de 2000.

BLAC00 Black, U. *IP Routing Protocols: RIP, OSPF, BGP, PNNI & Cisco Routing Protocols*. Upper Saddle River, NJ: Prentice Hall, 2000.

CARP02 Carpenter, B., y Nichols, K. «Differentiated Services in the Internet». *Proceedings of the IEEE*, septiembre de 2002.

CLAR92 Clark, D.; Shenker, S.; y Zhang, L «Supporting Real-Time Applications in an Integrated Services Packet Network: Architecture and Mechanism». *Proceedings, SIGCOMM'92*, agosto de 1992.

CLAR95 Clark, D. *Adding Service Discrimination to the Internet*. MIT Laboratory for Computer Science Technical Report, septiembre de 1995. disponible en http://anawww.lcs.mitedu/anaWeb/papers.html.

HARJ00 Harju, J., y Kivimaki, P. «Cooperation and Comparison of DiffServ and IntServ: Performance Measurements». *Proceedings, 23rd Annual IEEE Conference on Local Computer Networks*, noviembre de 2000.

HUIT00 Huitema, C. *Routing in the Internet*. Upper Saddle River, NJ: Prentice Hall, 2000.

KILK99 Kilkki, K. *Differentiated Services for the Internet*. Indianapolis, IN: Macmillan Technical Publishing, 1999.

KUMA98 Kumar, V.; Lakshman, T; y Stiliadis, D. «Beyond Best Effort: Router Architectures for the Differentiated Services of Tomorrow's Internet». *IEEE Communications Magazine*, mayo de 1998.

MOY98 Moy, J. *OSPF*: *Anatomy of an Internet Routing Protocol*. Reading, MA: Addison-Wesley, 1998.

PERL00 Perlman, R. *Interconnections*: *Bridges*, *Routers Switches*, *and Internetworking Protocols*. MA: Addison-Wesley, 2000.

SHEN95 Shenker, S. «Fundamental Design Issues for the Future Internet». *IEEE Journal on Selected Areas in Communications*, septiembre de 1995.

WEIS98 Weiss, W. «QoS with Differentiated Services». *Bell Labs Technical Journal*, octubre/diciembre de 1998.

WHIT97 White, P., y Crowcroft, J. «The Integrated Services in the Internet: State of the Art». *Proceedings of the IEEE*, diciembre de 1997.

XIAO99 Xiao, X., y Ni, L. «Internet QoS: A Big Picture». *IEEE Network*, marzo/abril de 1999.

ZHAN93 Zhang, L; Deering, S.; Estrim, D.; Shenker, S.; y Zappala, D. «RSVP: A New Resource ReSerVation Protocol». *IEEE Network*, septiembre de 1993.

ZHAN95 Zhang, H. «Service Disciplines for Guaranteed Performance Service in Packet-Switching Networks». *Proceeedings of the IEEE*, octubre de 1995.

SITIOS WEB RECOMENDADOS

- **Proyecto RSVP:** página de inicio del desarrollo de RSVP.
- **Grupo de trabajo de RSVP:** auspiciado por la IETF para desarrollar estándares relativos a servicios diferenciados. El sitio web incluye todos los RFC relacionados, así como los borradores para Internet.
- **Grupo de trabajo de OSPF:** auspiciado por la IETF para desarrollar OSPF y estándares relacionados. El sitio web incluye todos los RFC relacionados, así como los borradores para Internet.
- **Grupo de trabajo de servicios diferenciados:** auspiciado por la IETF para desarrollar estándares relativos a los servicios diferenciados. El sitio web incluye todos los RFC relacionados, así como los borradores para Internet.
- **Grupo de trabajo de servicios integrados:** auspiciado por la IETF para desarrollar estándares relativos a los servicios integrados. El sitio web incluye todos los RFC relacionados, así como los borradores para Internet.

19.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

adquisición de vecino
arquitectura de servicios integrados (ISA)
bloque de descarte de paquetes
calidad de servicio (QoS)
clasificador
comportamiento por salto (PHB)
conformador
detección de vecino alcanzable
detección de red alcanzable
dirección de difusión
dirección de multidifusión
dirección de unidifusión
disciplina de atención de cola
encaminamiento por estado de enlace
encaminamiento por vector camino
encaminamiento por vector distancia
marcador
monitor
multidifusión
protocolo del primer camino más corto disponible (OSPF)
protocolo de encaminador exterior (ERP)
protocolo de encaminador interior (IRP)
protocolo de gestión de grupos de Internet (IGMP)
protocolo de pasarela frontera (BGP)
protocolo de reserva de recursos (RSVP)
servicios diferenciados (DS)
sistema autónomo (AS)
tráfico elástico
tráfico inelástico
dispersión del retardo (*jitter*)

CUESTIONES DE REPASO

19.1. Enumere algunas aplicaciones prácticas de la multidifusión.

19.2. Resuma las diferencias existentes entre las direcciones de unidifusión, multidifusión y difusión.

19.3. Enumere y explique brevemente las funciones que se requieren para la multidifusión.

19.4. ¿Qué funciones realiza IGMP?

19.5. ¿Qué es un sistema autónomo?

19.6. ¿Cuál es la diferencia entre un protocolo de encaminador interior y un protocolo de encaminador exterior?

19.7. Compare las tres principales estrategias de encaminamiento.

19.8. Enumere y explique brevemente las tres funciones principales de BGP.

19.9. ¿Qué es la arquitectura de servicios integrados?

19.10. ¿Cuál es la diferencia que existe entre el tráfico elástico e inelástico?

19.11. ¿Cuáles son las funciones principales que forman parte de una ISA?

19.12. Enumere y describa brevemente las tres categorías de servicio ofrecidas por ISA.

19.13. ¿Cuál es la diferencia existente entre la disciplina de atención de cola FIFO y la WFQ?

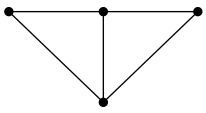
19.14. ¿Cuál es el propósito de un código DS?

19.15. Enumere y explique brevemente las cinco funciones principales del acondicionamiento de tráfico de DS.

19.16. ¿A qué se refiere el término «comportamiento por salto»?

EJERCICIOS

19.1. Un grafo conexo puede tener más de un árbol de expansión. Encuentre todos los árboles de expansión de este grafo:



19.2. En la discusión de la Figura 19.1, se comentan tres alternativas para transmitir un paquete a una dirección de multidifusión: difusión, unidifusión múltiple y multidifusión genuina. Otra posible alternativa es la inundación: la fuente transmite un paquete por todas las interfaces de salida, exceptuando aquella por la que el paquete ha sido recibido. Se etiqueta cada paquete con un identificador único de forma que un encaminador no inundará el mismo paquete más de una vez. Rellene una matriz similar a la de la Tabla 19.3 y comente los resultados.

19.3. De forma similar a la Figura 19.3, muestre los árboles de expansión que comiencen desde el encaminador B hasta el grupo de multidifusión.

19.4. IGMP especifica que los mensajes de consulta se envían en datagramas IP con el campo de tiempo de vida ajustado a 1. ¿Por qué?

19.5. Cuando existen múltiples rutas de igual coste a un destino, OSPF puede distribuir el tráfico de igual forma entre las rutas. Esto se llama *balanceado de carga*. ¿Qué efectos tiene este balanceado de carga en un protocolo de la capa de transporte, como es el caso de TCP?

19.6. Está claro que si un dispositivo de encaminamiento da trato preferencial a un flujo o a una clase de flujos, entonces ese flujo o clase de flujos recibirán un servicio mejorado. Pero no está tan claro que el servicio global que proporciona la interconexión de redes se mejore. Esta cuestión pretende ilustrar una mejora global. Considere una red con un solo enlace modelado por un servidor exponencial de tasa $T_s = 1$ y considere dos clases de flujos de Poisson con una tasa de llegada de $\lambda_1 = \lambda_1 = 0{,}25$, que tienen como funciones de utilización $U_1 = 4 - 2T_{q1}$ y $U_2 = 4 - T_{q2}$, donde T_{qi} representa el tiempo medio de estancia en cola para la clase i. Así pues, el tráfico de la clase 1 es más sensible al retardo que el de la clase 2. Defina la función de utilización total de la red como $V = U_1 + U_2$.

a) Suponga que las dos clases se tratan de forma diferente y que se utiliza la atención en cola FIFO. ¿Cuánto vale V?

b) Suponga ahora un servicio de prioridad estricto, de forma que los paquetes de la clase 1 sean siempre transmitidos antes que los paquetes de la clase 2. ¿Cuánto vale V? Comente el resultado.

19.7. El esquema de cubo de testigos establece un límite en la duración del tiempo en el que el tráfico puede transmitirse a la velocidad de transmisión máxima. Sean B octetos el tamaño del cubo de testigos, R octetos/segundo la tasa de llegada de testigos y M octetos/segundo la velocidad de transferencia máxima de salida.

a) Obtener una fórmula para S, la longitud de la ráfaga de velocidad máxima. Es decir, ¿durante cuánto tiempo puede un flujo transmitir a la velocidad máxima de salida cuando está controlado por un cubo de testigos?

b) ¿Cuál es el valor de S para $B = 250$ kB, $r = 2$ MB/s y $M = 25$ MB/s?

Sugerencia: la fórmula de S no es tan fácil como pudiera parecer, ya que llegan más testigos mientras la ráfaga se está enviando.

19.8. En RSVP, los números de puerto de UDP/TCP se utilizan para clasificar los paquetes, por lo que cada dispositivo de encaminamiento debe ser capaz de analizar estos campos. Esta necesidad trae problemas en las siguientes áreas:

a) Procesamiento de la cabecera IPv6.

b) Seguridad a nivel IP.

Indique la naturaleza del problema en cada área y sugiera una solución.

CAPÍTULO 20

Protocolos de transporte

20.1. Mecanismos de los protocolos de transporte orientados a conexión
Servicio de red de entrega ordenada fiable
Servicio de red no fiable

20.2. TCP
Servicios TCP
Formato de la cabecera TCP
Mecanismos TCP
Opciones en los criterios de implementación de TCP

20.3. Control de congestión de TCP
Gestión de temporizadores de retransmisión
Gestión de ventana

20.4. UDP

20.5. Lecturas recomendadas

20.6. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- El protocolo de transporte proporciona un servicio de transferencia de datos extremo a extremo que aísla las capas superiores de los detalles de la red o redes intermedios. Un protocolo de transporte puede ser orientado a conexión, como en el caso de TCP, o no orientado a conexión, como ocurre con UDP.
- Si el servicio de la red o interconexión subyacente no es fiable, como ocurre en el caso de IP, un protocolo fiable de transporte orientado a conexión resulta ser muy complejo. La causa básica de esta complejidad reside en la necesidad de tratar con los retardos variables y relativamente altos que se experimentan entre sistemas finales. Estos retardos complican las técnicas de control de flujo y de control de errores.
- TCP emplea una técnica de control de flujo basada en créditos que es, en cierta forma, diferente del control de flujo con ventana deslizante que encontramos en X.25 y HDLC. Básicamente, TCP separa las confirmaciones y la gestión del tamaño de la ventana deslizante.
- Aunque el mecanismo basado en créditos de TCP se diseñó para el control de flujo extremo a extremo, también se utiliza para ayudar en el control de congestión en las interconexiones de redes. Cuando una entidad TCP detecta la presencia de congestión en Internet, reduce el flujo de datos que envía por Internet hasta que detecta alivio en la congestión.

En una arquitectura de protocolos, el protocolo de transporte se sitúa sobre la capa de red o de interconexión, que proporciona los servicios relacionados con la red, y justo debajo de las capas de aplicación y de otros protocolos de capas superiores. El protocolo de transporte proporciona servicios a los usuarios del servicio de transporte (TS, *Transport Service*), como FTP, SMTP y TELNET. La entidad local de transporte se comunica con alguna otra entidad de transporte remota utilizando los servicios de alguna capa inferior, como puede ser el protocolo Internet (IP). El servicio general proporcionado por un protocolo de transporte es el transporte de datos extremo a extremo, de forma que aísle al usuario TS de los detalles de los sistemas de comunicaciones subyacentes.

Comenzaremos este capítulo analizando los mecanismos de protocolo que se requieren para proporcionar los servicios anteriormente citados. Encontraremos que la mayor parte de la complejidad se refiere a los servicios fiables orientados a conexión. Como cabría esperar, cuanto menos ofrece el servicio de red, más tareas debe realizar el protocolo de transporte. El resto del capítulo examina los dos protocolos de transporte más utilizados: el protocolo de control de transmisión (TCP, *Transmission Control Protocol*) y el protocolo de datagrama de usuario (UDP, *User Datagram Protocol*).

La Figura 2.15 destaca la posición de estos protocolos dentro del conjunto de protocolos TCP/IP.

20.1. MECANISMOS DE LOS PROTOCOLOS DE TRANSPORTE ORIENTADOS A CONEXIÓN

Son posibles dos tipos básicos de servicio de transporte: orientado a conexión y no orientado a conexión o servicio de datagramas. Un servicio orientado a conexión proporciona el establecimiento, mantenimiento y cierre de una conexión lógica entre usuarios de TS. Éste ha sido hasta ahora el

tipo de servicio de protocolo más utilizado y tiene una gran variedad de aplicaciones. El servicio orientado a conexión implica generalmente que el servicio es fiable. Esta sección examina los mecanismos del protocolo de transporte necesarios para ofrecer un servicio orientado a conexión.

Un protocolo de transporte orientado a conexión completo, como TCP, es muy complejo. Por motivos de claridad, presentamos los mecanismos del protocolo de transporte de forma incremental. Empezaremos con un servicio de red que facilite el funcionamiento del protocolo de transporte garantizando la entrega en orden de todas las unidades de datos de transporte y definiendo los mecanismos requeridos. Después examinaremos los mecanismos de protocolo de transporte requeridos para hacer frente a un servicio de red no fiable. Toda esta discusión se aplica en general a los protocolos de la capa de transporte. En la Sección 20.2, aplicaremos los conceptos desarrollados en esta sección para describir TCP.

SERVICIO DE RED DE ENTREGA ORDENADA FIABLE

Supongamos que el servicio de red acepta mensajes de tamaño arbitrario y que, con prácticamente una fiabilidad del 100 por cien, los entrega en secuencia al destino. Algunos ejemplos de estas redes son:

- Una red de conmutación de paquetes altamente fiable con una interfaz X.25.
- Una red de retransmisión de tramas que utilice el protocolo de control LAPF.
- Una LAN IEEE 802.3 que utilice el servicio LLC orientado a conexión.

En todos esos casos, el protocolo de transporte se utiliza como un protocolo extremo a extremo entre dos sistemas finales conectados a la misma red, en lugar de hacerlo a través de una interconexión de red.

La suposición de servicios de red con entrega en orden fiable permite el uso de un protocolo de transporte bastante sencillo. Hay cuatro cuestiones a considerar:

- Direccionamiento.
- Multiplexación.
- Control de flujo.
- Establecimiento/cierre de la conexión.

Direccionamiento

La cuestión sobre el direccionamiento es simplemente ésta: un usuario de una entidad de transporte dada desea, bien establecer una conexión, o bien realizar una transferencia de datos con un usuario de alguna otra entidad de transporte que utilice el mismo protocolo de transporte. Es necesario que se identifique al usuario destino mediante toda la información siguiente:

- Identificación del usuario.
- Identificación de la entidad de transporte.
- Dirección de la estación.
- Número de la red.

El protocolo de transporte debe ser capaz de extraer de la dirección del usuario TS la información indicada anteriormente. Normalmente, la dirección de usuario se especifica como (*estación*, *puerto*). La variable *puerto* representa un usuario TS particular en la estación especificada. En general,

existirá una sola entidad de transporte en cada estación, por lo que no se necesita una identificación de la entidad. Si más de una entidad de transporte está presente, normalmente hay una de cada tipo. En este último caso, la dirección debe incluir una indicación del tipo de protocolo de transporte (por ejemplo, TCP o UDP). En el caso de una única red, la *estación* identifica a un dispositivo de red conectado a la misma. En el caso de un conjunto de redes interconectadas, *estación* es una dirección global de red. En TCP, la combinación del puerto y la estación se denomina *socket*.

Ya que el encaminamiento no es una cuestión de la capa de transporte, ésta simplemente pasa la parte de la dirección *estación* al servicio de red. El campo *puerto* se incluye en una cabecera de transporte para que la entidad del protocolo de transporte destino la utilice.

Queda todavía una cuestión por abordar: ¿cómo puede el usuario TS que inicia la comunicación conocer la dirección del usuario TS destino? Existen dos estrategias estáticas y dos dinámicas que se explican por sí mismas:

1. El usuario TS previamente conoce la dirección que desea utilizar. Ésta es básicamente una función de configuración del sistema. Por ejemplo, puede estar ejecutándose un proceso que sólo interese a un número limitado de usuarios TS, como por ejemplo un proceso que recoja estadísticas sobre prestaciones. De vez en cuando, una rutina de gestión de red central se conecta al proceso para obtener las estadísticas. En general, estos procesos no son, y no deben ser, bien conocidos ni accesibles por todos.
2. A algunos servicios usados comúnmente se le asignan direcciones bien conocidas. Por ejemplo, servidores de FTP, SMTP y algunos otros protocolos estándares.
3. Proporcionando un servidor de nombres. El usuario TS solicita un servicio mediante algún nombre genérico o global. Esta petición se envía a un servidor de nombres, que realiza una búsqueda en un directorio y devuelve una dirección. La entidad de transporte procede entonces con la conexión. Este servicio es útil para aplicaciones comunes que cambien su localización de vez en cuando. Por ejemplo, un proceso de entrada de datos se podría cambiar de una estación a otra en una red local para balancear la carga.
4. En algunos casos, el usuario destino es un proceso creado en el momento de la solicitud. El usuario que inicia la comunicación puede enviar una solicitud a una dirección bien conocida. El usuario en esa dirección es un proceso del sistema con privilegios que genera al nuevo proceso y devuelve una dirección. Por ejemplo, un programador ha desarrollado una aplicación privada (por ejemplo, un programa de simulación) que se ejecutará en un servidor remoto, pero que será invocado desde una estación de trabajo local. Se puede mandar una petición a un proceso de gestión de trabajos remoto para que lance el proceso de simulación.

Multiplexación

El concepto de multiplexación se discutió en términos generales en la Sección 18.1. Con respecto a la interfaz entre el protocolo de transporte y los protocolos de capas superiores, el protocolo de transporte lleva a cabo una función de multiplexado/demultiplexado. Es decir, múltiples usuarios emplean el mismo protocolo de transporte, distinguiéndose unos de otros mediante números de puerto o puntos de acceso al servicio.

La entidad de transporte también puede llevar a cabo una función de multiplexación con respecto a los servicios de red que usa. Recuerde que definimos multiplexación hacia arriba como la multiplexación de múltiples conexiones sobre una única conexión de la capa inferior y multiplexa-

ción hacia abajo como la división de una única conexión entre múltiples conexiones de capas inferiores.

Por ejemplo, considere una entidad de transporte que haga uso de un servicio de X.25. ¿Por qué debería una entidad de transporte emplear multiplexación hacia arriba? Después de todo, hay 4.095 circuitos virtuales disponibles. En el caso típico, esto es más que suficiente para gestionar todos los usuarios TS activos. Sin embargo, la mayoría de las redes X.25 basan parte de su tarificación en el tiempo de conexión del circuito virtual, ya que cada circuito virtual consume algunos recursos de memoria temporal del nodo. Por ello, si un solo circuito virtual proporciona el rendimiento suficiente para varios usuarios TS, es indicado utilizar multiplexación hacia arriba.

Por otra parte, la división o multiplexación hacia abajo se podría emplear para mejorar el rendimiento. Por ejemplo, cada circuito virtual X.25 está restringido a un número de secuencia de 3 o 7 bits. Para redes de alta velocidad y gran retardo podría requerirse un mayor espacio de números de secuencia. Por supuesto, el rendimiento sólo se puede incrementar hasta este nivel. Si sólo existe un único enlace estación-nodo sobre el cual se multiplexan todos los circuitos virtuales, el rendimiento de una conexión de transporte no puede exceder la velocidad de transmisión de datos de ese enlace.

Control de flujo

Mientras que el control de flujo es un mecanismo relativamente sencillo en la capa de enlace, en la capa de transporte constituye un mecanismo bastante complejo por dos razones principales:

- El retardo de transmisión entre entidades de transporte es generalmente grande comparado con el tiempo de transmisión real. Esto significa que existe un retardo considerable en la comunicación de la información de control de flujo.
- Ya que la capa de transporte opera sobre una red o una interconexión de redes, la cantidad de retardo en la transmisión puede ser muy variable. Esto hace difícil utilizar de forma efectiva un mecanismo de tiempos de expiración para la retransmisión de datos perdidos.

En general existen dos razones por las que una entidad de transporte querría moderar la tasa de transmisiones de segmentos[1] sobre una conexión de otra entidad de transporte:

- Que el usuario de la entidad de transporte receptora no pueda mantener la tasa del flujo de datos que recibe.
- Que la propia entidad de transporte receptora no pueda mantener la tasa del flujo de segmentos.

¿Cómo se manifiestan los problemas mencionados? Presumiblemente, una entidad de transporte tiene una cierta capacidad de memoria temporal. Los segmentos que se reciben se almacenan en esa memoria. Cada segmento almacenado es procesado (es decir, se examina su cabecera de transporte) y los datos se envían al usuario de TS. Cualquiera de los dos problemas mencionados antes causará que la memoria temporal se llene. Por ello, la entidad de transporte necesita tomar medidas para detener o disminuir el flujo de segmentos con objeto de evitar el desbordamiento de la memoria temporal. Este requisito es difícil de cumplir a causa del molesto intervalo de tiempo que hay entre el emisor y el receptor. Volveremos a este punto más adelante. Primero, vamos a presentar cuatro formas de hacer frente al requisito de control de flujo. La entidad de transporte receptora puede:

[1] Recuerde del Capítulo 2 que los bloques de datos (unidades de datos del protocolo) intercambiados por las entidades TCP se denominan segmentos TCP.

1. No hacer nada.
2. Rechazar la aceptación de más segmentos del servicio de red.
3. Usar un protocolo de ventana deslizante fija.
4. Usar un esquema de créditos.

La alternativa 1 significa que los segmentos que desborden la memoria temporal serán descartados. La entidad de transporte emisora, al no obtener una confirmación, los retransmitirá. Esto es inaceptable, ya que la ventaja de una red fiable es que uno nunca tiene que retransmitir. Es más, el efecto de esta maniobra es que se agrava el problema: el emisor incrementa sus envíos para incluir nuevos segmentos además de los antiguos.

La segunda alternativa es un mecanismo de contrapresión que se basa en el servicio de red para hacer el trabajo. Cuando una memoria temporal de una entidad de transporte está llena, esta entidad rechaza datos adicionales del servicio de red. Esto dispara los procedimientos de control de flujo dentro de la red que regulan el servicio de red en el extremo del emisor. En respuesta, este servicio rechaza segmentos adicionales de su entidad de transporte. Debe quedar claro que este mecanismo es poco preciso y tosco. Por ejemplo, si varias conexiones de transporte se multiplexan sobre una única conexión de red (circuito virtual), el control de flujo se ejerce sólo sobre el agregado de todas las conexiones de transporte.

La tercera estrategia resultará familiar al lector del análisis sobre los protocolos de la capa de enlace del Capítulo 7. Recuerde que los ingredientes clave son:

- El empleo de números de secuencia en las unidades de datos.
- El empleo de una ventana de tamaño fijo.
- El empleo de confirmaciones para avanzar la ventana.

Con un servicio de red fiable, la técnica de ventana deslizante funcionaría realmente bien. Por ejemplo, considere un protocolo con un tamaño de ventana de 7. Cuando el emisor recibe una confirmación de un segmento particular, se le autoriza automáticamente a enviar los siete segmentos siguientes (por supuesto, algunos pueden haber sido ya enviados). Cuando la capacidad de la memoria temporal del receptor disminuya a 7 segmentos, el receptor puede retener las confirmaciones de los segmentos que reciba para evitar el desbordamiento. La entidad de transporte emisora puede enviar como mucho siete segmentos adicionales y después debe dejar de enviar. Como el servicio de red subyacente es fiable, los temporizadores del emisor no expirarán ni habrá retransmisión. Así, en algún punto, una entidad de transporte emisora puede tener varios segmentos pendientes para las cuales no se ha recibido confirmación. Ya que trabajamos con una red fiable, la entidad de transporte emisora puede suponer que los segmentos se han entregado y que la ausencia de confirmaciones es debida a una táctica de control de flujo. Esta táctica no funcionará bien en una red no fiable, ya que la entidad de transporte emisora no sabría si la falta de confirmaciones se debe al control de flujo o a la pérdida de un segmento.

La cuarta alternativa, un esquema de créditos, proporciona al receptor un mayor grado de control sobre el flujo de datos. Aunque no es estrictamente necesario con un servicio de red fiable, un esquema de créditos debe dar lugar a un flujo de tráfico más fluido. Además, es un esquema más efectivo con un servicio de red no fiable, como veremos.

El esquema de créditos desliga las confirmaciones y el control de flujo. En los protocolos de ventana deslizante fija, como X.25, los dos conceptos son sinónimos. En un esquema de créditos, se puede confirmar un segmento sin la concesión de nuevo crédito y viceversa. En el esquema de créditos se considera que cada octeto individual de datos que se transmite tiene un número de

secuencia único. Además de los datos, cada segmento transmitido incluye en su cabecera tres campos relacionados con el control de flujo: el número de secuencia (*SN*), el número de confirmación (*AN*) y la ventana (*W*). Cuando una entidad de transporte envía un segmento, incluye el número de secuencia del primer octeto del campo de datos del segmento. Una entidad de transporte confirma un segmento recibido con un segmento de retorno que incluye ($AN = i$, $W = j$), con la siguiente interpretación:

- Todos los octetos cuyos números de secuencia lleguen hasta $SN = i - 1$ se confirman. El siguiente octeto esperado tiene número de secuencia i.
- Se concede permiso para enviar una ventana adicional de $W = j$ octetos de datos. Es decir, los j octetos correspondientes a los números de secuencia desde i hasta $i + j - 1$.

La Figura 20.1 ilustra este mecanismo (compárese con la Figura 7.4). Por simplicidad, se muestra el flujo de datos en un solo sentido y se supone que en cada segmento se envían 200 octetos. Inicialmente, a través del proceso de establecimiento de la conexión, se sincronizan los números de secuencia de emisión y recepción y A obtiene una asignación inicial de 1.400 octetos, comenzando con el octeto número 1.001. Después de enviar 600 octetos en tres segmentos, A ha reducido su ventana a un tamaño de 800 octetos (números del 1.601 al 2.400). Después de que B reciba esos tres segmentos, se contabilizan 600 octetos de los 1.400 originales de crédito, quedando pendientes 800 créditos. Suponga ahora que, llegados a este punto, B es capaz de absorber 1.000 octetos de datos provenientes de esta conexión. De acuerdo a esto, B confirma la recepción de todos los octetos hasta 1.600 y emite un crédito de 1.000 octetos. Esto significa que A puede enviar los octetos comprendidos entre 1.601 y 2.600 (5 segmentos). Sin embargo, cuando el mensaje de B haya llegado a A, A ya habrá enviado dos segmentos, que contienen los octetos del 1.601 al 2.000 (lo cual se permitía según la reserva inicial). Así, el crédito restante de A tras la recepción de la cuota de crédito de B es sólo de 600 octetos (3 segmentos). Conforme el intercambio prosigue, A avanza el borde final de su ventana cada vez que transmite y avanza el borde inicial sólo cuando se le concede crédito.

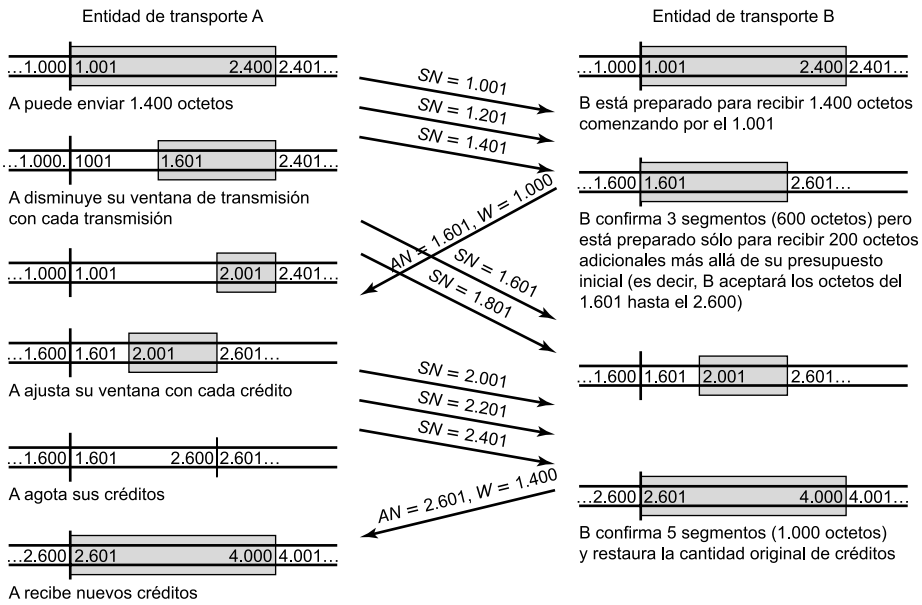

Entidad de transporte A
Entidad de transporte B
...1.000 1.001 2.400 2.401...
A puede enviar 1.400 octetos
SN = 1.001
SN = 1.201
SN = 1.401
B está preparado para recibir 1.400 octetos comenzando por el 1.001
...1.000. 1001 1.601 2.401...
A disminuye su ventana de transmisión con cada transmisión
...1.600 1.601 2.601...
B confirma 3 segmentos (600 octetos) pero está preparado sólo para recibir 200 octetos adicionales más allá de su presupuesto inicial (es decir, B aceptará los octetos del 1.601 hasta el 2.600)
AN = 1.601, W = 1.000
SN = 1.601
SN = 1.801
...1.000 1.001 2.001 2.401...
...1.600 1.601 2.001 2.601...
A ajusta su ventana con cada crédito
SN = 2.001
SN = 2.201
SN = 2.401
...1.600 1.601 2.600 2.601...
A agota sus créditos
AN = 2.601, W = 1.400
...2.600 2.601 4.000 4.001...
B confirma 5 segmentos (1.000 octetos) y restaura la cantidad original de créditos
...2.600 2.601 4.000 4.001...
A recibe nuevos créditos

Figura 20.1. Ejemplo del mecanismo de asignación de crédito de TCP.

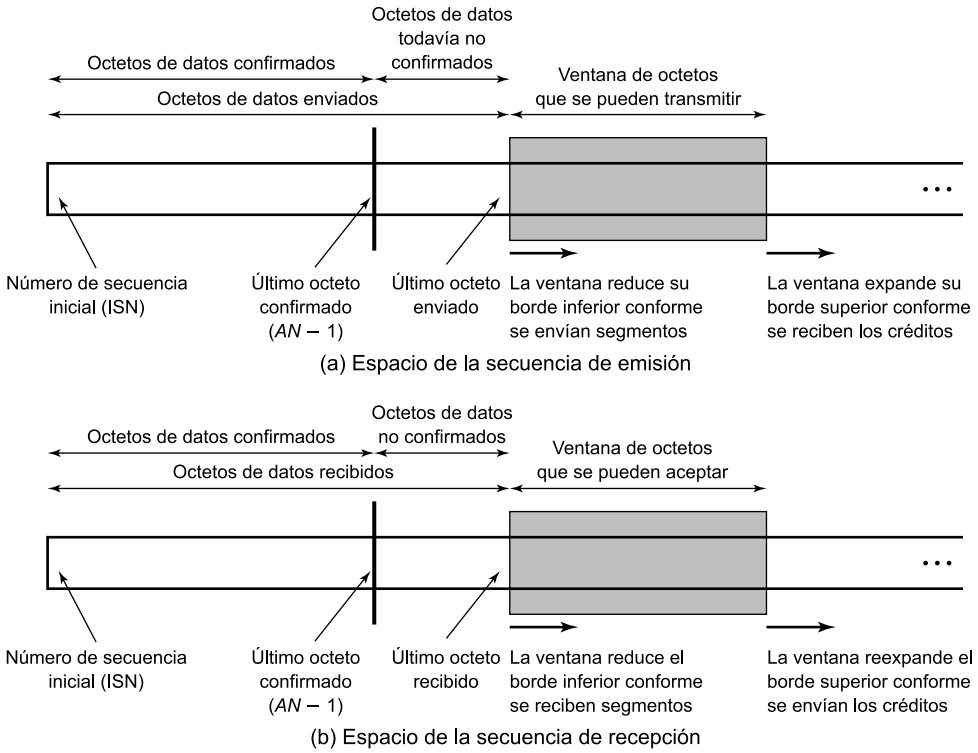

Octetos de datos todavía no confirmados
Octetos de datos confirmados
Octetos de datos enviados
Ventana de octetos que se pueden transmitir
Número de secuencia inicial (ISN)
Último octeto confirmado (AN − 1)
Último octeto enviado
La ventana reduce su borde inferior conforme se envían segmentos
La ventana expande su borde superior conforme se reciben los créditos
(a) Espacio de la secuencia de emisión
Octetos de datos no confirmados
Octetos de datos confirmados
Octetos de datos recibidos
Ventana de octetos que se pueden aceptar
Número de secuencia inicial (ISN)
Último octeto confirmado (AN − 1)
Último octeto recibido
La ventana reduce el borde inferior conforme se reciben segmentos
La ventana reexpande el borde superior conforme se envían los créditos
(b) Espacio de la secuencia de recepción

Figura 20.2. Perspectivas del control de flujo en el envío y en la recepción.

La Figura 20.2 muestra una visión de este mecanismo según el emisor y según el receptor (compárese con la Figura 7.3). Normalmente, ambos extremos tienen ambas perspectivas, ya que los datos se pueden intercambiar en ambos sentidos. Observe que no se requiere que el receptor confirme inmediatamente los segmentos recibidos, sino que puede esperar y emitir una confirmación acumulada para varios segmentos.

El receptor necesita adoptar alguna política sobre la cantidad de datos que le va a permitir transmitir al emisor. La opción conservadora consiste en permitir sólo nuevos segmentos hasta el límite del espacio de memoria temporal disponible. Si esta política fuera la utilizada en la Figura 20.1, el primer mensaje de crédito implica que B dispone de 1.000 octetos en su memoria temporal y el segundo mensaje, que B tiene 1.400 octetos disponibles.

Un esquema de control de flujo conservador puede limitar el rendimiento de la conexión de transporte en situaciones de gran retardo. El receptor podría incrementar potencialmente el rendimiento mediante la concesión de forma optimista de créditos de espacio que no tiene. Por ejemplo, si la memoria temporal del receptor está llena, pero anticipa que puede liberar el espacio para 1.000 octetos dentro del tiempo de propagación de ida y vuelta, podría enviar inmediatamente un crédito de 1.000 octetos. Si el receptor puede ir al paso del emisor, este esquema podría incrementar el rendimiento sin causar perjuicio alguno. Sin embargo, si el emisor es más rápido que el receptor, algunos segmentos pueden ser descartados, necesitando una retransmisión. Ya que las retransmisiones no son necesarias en otro caso con un servicio de red fiable (en ausencia de congestión en la interconexión de redes), un esquema optimista de control de flujo complicará el protocolo.

Establecimiento y cierre de la conexión

Incluso con un servicio de red fiable, existe la necesidad de procedimientos de establecimiento y cierre de conexión para ofrecer un servicio orientado a conexión. El establecimiento de la conexión cumple tres objetivos principales:

- Permite a cada extremo asegurarse de que el otro existe.
- Permite el intercambio o negociación de parámetros opcionales (por ejemplo, el tamaño máximo del segmento, el tamaño máximo de la ventana y la calidad de servicio).
- Inicia la reserva de recursos de la entidad de transporte (por ejemplo, espacio de memoria temporal y entradas en la tabla de conexiones).

El establecimiento de la conexión se realiza por mutuo acuerdo, pudiéndose llevar a cabo mediante un conjunto sencillo de órdenes de usuario y segmentos de control, como se muestra en el diagrama de estados de la Figura 20.3. Para comenzar, un usuario TS está en un estado *CLOSED* («CERRADO», es decir, no tiene una conexión de transporte abierta). El usuario TS puede indicar a la entidad TCP local que esperará de forma pasiva una solicitud con una orden de *Passive Open* («apertura pasiva»). Esto es lo que podría hacer un programa servidor, como una aplicación de tiempo compartido o una aplicación de transferencia de ficheros. El usuario TS puede cambiar de idea enviando una orden *Close* («cerrar»). Después de haberse emitido la orden *Passive Open*, la entidad de transporte crea un objeto de conexión de algún tipo (es decir, una entrada en una tabla) que está en el estado *LISTEN* («PREPARADO»).

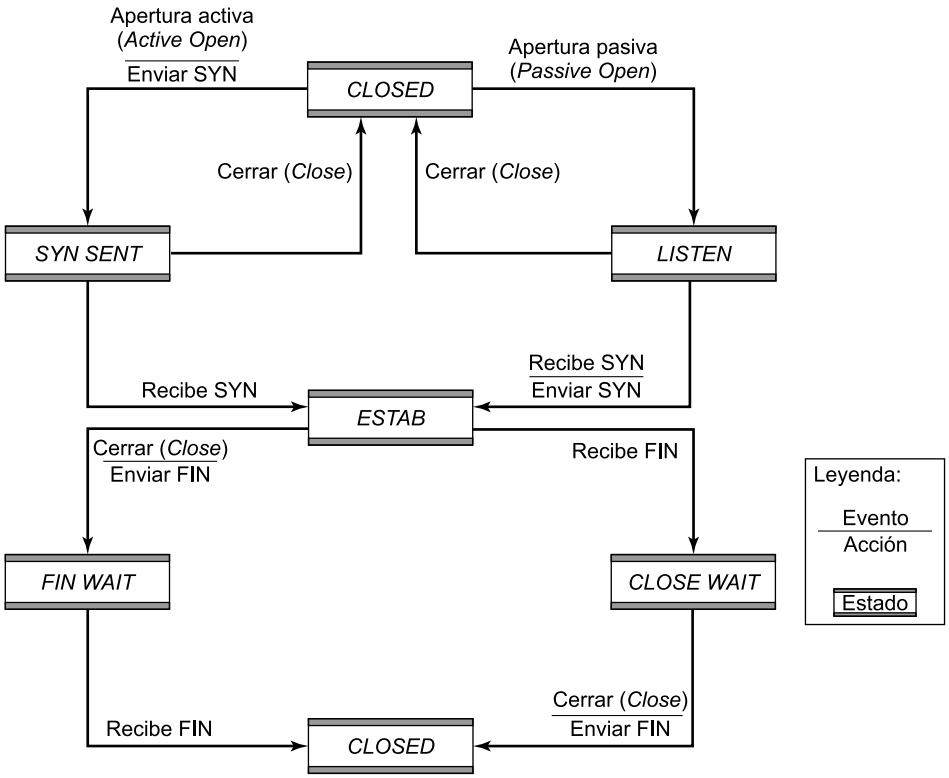


Figura 20.3. Diagrama de estados de la conexión simple.

Desde el estado *CLOSED*, el usuario TS puede abrir una conexión emitiendo una orden *Passive Open*, la cual instruye a la entidad de transporte para que intente establecer una conexión con un usuario TS remoto designado, lo que hace que la entidad de transporte envíe un segmento SYN (para sincronizar). El segmento se entrega a la entidad de transporte receptora, donde se interpreta como una solicitud de conexión a un puerto concreto. Si la entidad de transporte destino está en el estado LISTEN para ese puerto, entonces se establece una conexión por medio de las acciones siguientes, realizadas por la entidad de transporte receptora:

- Informa al usuario TS local que una conexión está abierta.
- Envía un segmento SYN como confirmación a la entidad de transporte remota.
- Sitúa el objeto de conexión en el estado ESTAB (establecida).

Cuando el segmento SYN de respuesta lo recibe la entidad de transporte que inició el proceso, ella también puede pasar la conexión al estado ESTAB. La conexión se interrumpe prematuramente si cualquier usuario TS emite una orden *Close*.

La Figura 20.4 muestra la robustez de este protocolo. Cualquier extremo puede iniciar una conexión. Además, si ambas partes inician la conexión en instantes próximos, ésta se establece sin confusión. Esto es así porque el segmento SYN funciona como petición y como confirmación de la conexión.

El lector se puede preguntar qué ocurre si llega un segmento SYN en un momento en el que el usuario TS solicitado esta inactivo (no atendiendo peticiones). Se pueden seguir tres alternativas:

- La entidad de transporte puede rechazar la petición enviando un segmento RST («reiniciar») a la otra entidad de transporte.
- La solicitud se puede poner en cola hasta que el usuario TS local emita una orden *Open* («abrir») correspondiente.
- La entidad de transporte puede interrumpir al usuario TS local para notificarle una solicitud pendiente.

Observe que si se utiliza este último mecanismo, no es estrictamente necesaria una orden *Passive Open*, sino que se podría sustituir por una orden *Accept* («aceptar»), que es una señal del usuario utilizada para indicarle a la entidad de transporte que acepta la solicitud de conexión.

El cierre de la conexión se trata de manera similar. Pueden iniciar el cierre cualquiera de los extremos, o ambos a la vez. La conexión se cierra por mutuo acuerdo. Esta estrategia permite un

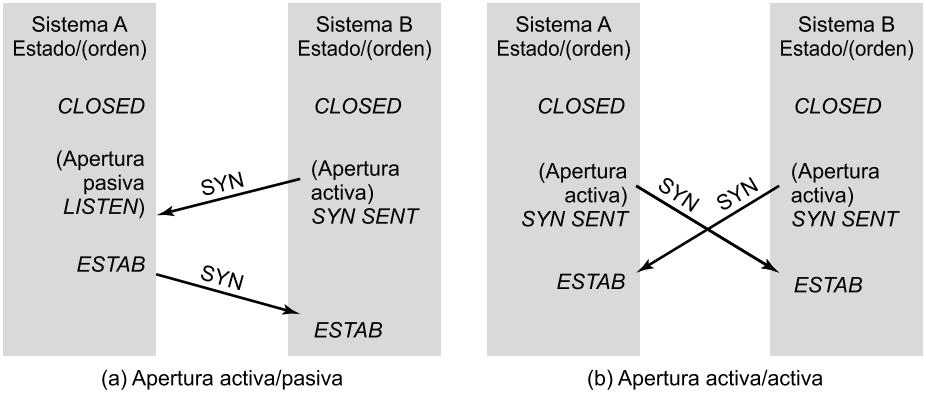


Figura 20.4. Escenarios de establecimiento de la conexión.

cierre abrupto u ordenado. En un cierre abrupto, los datos en tránsito pueden perderse. Un cierre ordenado impide a ambas partes cerrar la conexión hasta que todos los datos hayan sido entregados. Para conseguir esto último, una conexión que está en el estado *FIN WAIT* («ESPERA CIERRE») debe continuar aceptando segmentos de datos hasta que se reciba un segmento FIN («finalizar»).

La Figura 20.3 muestra el procedimiento para un cierre ordenado. Primero, consideremos el extremo que inicia el proceso de cierre:

1. En respuesta a una primitiva *Close* del usuario TS, la entidad de transporte envía un segmento FIN al otro extremo de la conexión, solicitando el cierre.
2. Habiendo enviado el segmento FIN, la entidad de transporte sitúa la conexión en el estado FIN WAIT. En este estado, la entidad de transporte debe continuar aceptando datos del otro extremo y entregarlos a su usuario.
3. Cuando se recibe como respuesta un segmento FIN, la entidad de transporte informa a su usuario y cierra la conexión.

Desde el punto de vista del extremo que no inicia el cierre:

1. Cuando se recibe un segmento FIN, la entidad de transporte informa a su usuario de la solicitud de cierre y sitúa la conexión en el estado *CLOSE WAIT* («ESPERA CIERRE»). En este estado, la entidad de transporte debe continuar aceptando datos de su usuario y transmitirlos en segmentos de datos al otro extremo.
2. Cuando el usuario emite una primitiva *Close*, la entidad de transporte envía un segmento FIN de respuesta al otro extremo y cierra la conexión.

Este procedimiento asegura que ambos extremos han recibido todos los datos pendientes y que ambos están de acuerdo en terminar la conexión antes del cierre real.

SERVICIO DE RED NO FIABLE

Un caso más difícil para un protocolo de transporte es aquel en que se ofrece un servicio de red no fiable. Ejemplos de tales redes son:

- Una interconexión de redes que utilice IP.
- Una red de retransmisión de tramas que utilice sólo el núcleo del protocolo LAPF.
- Una LAN IEEE 802.3 que use un servicio LLC no orientado a conexión sin confirmaciones.

El problema no consiste sólo en que los segmentos puedan perderse ocasionalmente, sino en que los segmentos pueden no llegar en secuencia debido al retardo variable del tránsito. Como veremos, se necesita un elaborado mecanismo para hacer frente a esas dos deficiencias interrelacionadas de la red. También veremos que se produce un patrón desalentador. La combinación de desorden y ausencia de fiabilidad genera problemas con todos los mecanismos que hemos discutido hasta ahora. Generalmente, la solución a cada problema produce nuevos problemas. Aunque hay problemas que tienen que ser resueltos por los protocolos en todas las capas, parece que existen más dificultades en un protocolo de transporte orientado a conexión fiable que en cualquier otro tipo de protocolo.

En el resto del esta sección, a menos que se indique expresamente, los mecanismos que se tratan son aquellos que utiliza TCP. Siete cuestiones han de ser tratadas:

- Entrega ordenada.
- Estrategia de retransmisión.
- Detección de duplicados.
- Control de flujo.
- Establecimiento de la conexión.
- Cierre de la conexión.
- Recuperación ante fallos.

Entrega ordenada

Con un servicio de red no fiable, es posible que los segmentos, incluso en el caso de que lleguen todos, lo hagan de forma desordenada. La solución a este problema consiste en numerar los segmentos secuencialmente. Ya hemos visto que para los protocolos de control del enlace de datos, como HDLC o X.25, cada unidad de datos (trama, paquete) se numera secuencialmente, siendo cada número de secuencia sucesivo mayor en una unidad que el número de secuencia precedente. Este esquema se utiliza en algunos protocolos de transporte, como los protocolos de transporte de ISO. Sin embargo, TCP usa un esquema algo diferente en el que cada octeto de datos que se transmite se numera implícitamente. Así, el primer segmento puede tener el número de secuencia igual a 1. Si ese segmento contiene 200 octetos de datos, entonces el segundo segmento tendría el número de secuencia 201 y así sucesivamente. Por simplicidad, en las discusiones de esta sección supondremos que el número de secuencia de cada segmento sucesivo es 200 más que el del segmento previo, es decir, cada segmento contiene exactamente 200 octetos de datos.

Estrategia de retransmisión

Existen dos eventos que requieren la retransmisión de un segmento. En primer lugar, el segmento se puede dañar en el camino, pero llegar sin embargo a su destino. Si se incluye en el segmento una suma de comprobación, la entidad de transporte receptora puede detectar el error y descartar el segmento. La segunda contingencia consiste en que el segmento no llegue a su destino. En cualquier caso, la entidad de transporte emisora no sabe que la transmisión del segmento no se ha realizado con éxito. Para tratar esta contingencia se utiliza un esquema de confirmaciones positivas: el receptor debe confirmar cada segmento recibido satisfactoriamente devolviendo un segmento que contenga un número de confirmación. Por razones de eficiencia, no se requiere una confirmación por cada segmento. En su lugar, puede utilizarse una confirmación acumulada, como se ha visto ya varias veces en este libro. Así, el receptor puede recibir los segmentos numerados como 1, 201 y 401, pero sólo envía $AN = 601$ de vuelta. El emisor debe interpretar $AN = 601$ como que los segmentos con $SN = 401$ y anteriores se han recibido correctamente.

Si un segmento no llega con éxito, no se enviará una confirmación positiva y se tendrá que efectuar una retransmisión. Para poder hacer frente a esta situación, tiene que haber un temporizador asociado con cada segmento conforme se envía. Si el temporizador expira antes de que se confirme, el emisor debe retransmitir el segmento asociado.

Así pues, la inclusión de temporizadores soluciona ese problema. Siguiente problema: ¿qué valor debe asignarse al temporizador? Existen dos estrategias que surgen por sí mismas. Se podría utilizar un temporizador con un valor fijo, basado en la comprensión del comportamiento típico de la red. Esta estrategia adolece de incapacidad para reaccionar ante los cambios en las condiciones

de la red. Si el valor es demasiado bajo, habrá muchas retransmisiones innecesarias, desperdiciando la capacidad de la red. Si el valor es demasiado alto, el protocolo será muy lento en reaccionar ante la pérdida de un segmento. El temporizador debe fijarse a un valor un poco mayor que el retardo de ida y vuelta (tiempo de enviar un segmento y recibir un ACK). Por supuesto, este retardo es variable incluso para una carga constante de la red. Y lo que es peor, la estadística del retardo variará con las cambiantes condiciones de la red.

La otra estrategia es utilizar un esquema adaptable, el cual tiene sus propios problemas. Supongamos que la entidad de transporte registra el tiempo que se tarda en confirmar los segmentos de datos y fija los temporizadores de retransmisión de acuerdo a la media de los retardos observados. No es posible confiar en este valor por tres razones:

- La entidad de transporte par puede que no confirme inmediatamente un segmento. Recordemos que le hemos dado el privilegio de utilizar confirmaciones acumuladas.
- Si un segmento ha sido retransmitido, el emisor no puede saber si la confirmación positiva recibida es una respuesta a la transmisión inicial o a la retransmisión.
- Las condiciones de la red pueden cambiar de repente.

Cada uno de estos problemas es la causa de alguna complicación adicional del algoritmo de transporte, pero el problema no admite una solución completa. Siempre habrá alguna incertidumbre con respecto al mejor valor para el temporizador de retransmisión.

Por cierto, el temporizador de retransmisión es sólo uno de varios temporizadores necesarios para el correcto funcionamiento del protocolo de transporte. Estos se listan en la Tabla 20.1, junto a una breve explicación.

Tabla 20.1. Temporizadores del protocolo de transporte.

Temporizador de retransmisión	Para retransmitir un segmento no confirmado.
Temporizador de reconexión	Tiempo mínimo entre el cierre de una conexión y el establecimiento de otra con la misma dirección destino.
Temporizador de ventana	Tiempo máximo entre segmentos ACK/CREDIT.
Temporizador de retransmisión de SYN	Intervalo de tiempo entre intentos de establecimiento de una conexión.
Temporizador de persistencia	Utilizado para abortar una conexión cuando no se confirma ningún segmento.
Temporizador de inactividad	Utilizado para abortar una conexión cuando no se recibe ningún segmento.

Detección de duplicados

Si se pierde un segmento y después se retransmite, no se producirá ninguna confusión. Sin embargo, si uno o más segmentos sucesivos se entregan satisfactoriamente pero se pierde el correspondiente ACK, expirará el temporizador de la entidad de transporte emisora y se retransmitirán uno o más segmentos. Si esos segmentos retransmitidos llegan correctamente, se tendrán duplicados de los segmentos anteriormente recibidos. Por ello, el receptor debe ser capaz de reconocer los duplicados. El hecho de que cada segmento lleve un número de secuencia ayuda, pero, de cualquier forma, la detección y gestión de los duplicados no es una tarea fácil. Existen dos casos:

- Se recibe un duplicado antes del cierre de la conexión.
- Se recibe un duplicado después de que se haya cerrado la conexión.

El segundo caso se estudia en la sección acerca del establecimiento de la conexión. Aquí trataremos el primer caso.

Observe que decimos «un» duplicado y no «el» duplicado. Desde el punto de vista del emisor, el segmento retransmitido es el duplicado. Sin embargo, el segmento retransmitido puede llegar antes que el segmento original, en cuyo caso el receptor vería el segmento original como el duplicado. En cualquier caso, se necesitan dos tácticas para tratar el caso de que un duplicado se reciba antes de cerrar una conexión:

- El receptor debe asumir que su confirmación se perdió y, por tanto, debe confirmar el duplicado. Por consiguiente, el emisor debe no confundirse si recibe varias confirmaciones positivas del mismo segmento.
- El espacio de números de secuencia debe ser lo suficientemente amplio para no agotarse antes del tiempo máximo de vida posible de un segmento (tiempo que necesita el segmento para atravesar la red).

La Figura 20.5 ilustra la justificación de este último requisito. En este ejemplo, el espacio de secuencia es de longitud 1.600. Es decir, después de $SN = 1.600$, los números de secuencia vuelven a empezar con $SN = 1$. Por simplicidad, suponemos que la entidad de transporte receptora mantiene una ventana de crédito de tamaño 600. Suponga que A ha transmitido los segmentos de datos con $SN = 1$, 201 y 401. B ha recibido los dos segmentos con $SN = 201$ y 401, pero el segmento con el $SN = 1$ se ha retrasado en el camino. De esta forma, B no envía ninguna confirmación. Eventualmente, el temporizador de A expira y retransmite el segmento $SN = 1$. Cuando llega el duplicado del segmento $SN = 1$, B confirma el 1, el 201 y el 401 con $AN = 601$. Mientras tanto, en A se produce otra expiración y retransmite el $SN = 201$, que confirma B con otro $AN = 601$. Parece que las cosas se han arreglado solas y la transferencia de datos continúa. Cuando el espacio de secuencia se agota, A vuelve a comenzar con el número de secuencia $SN = 1$ y continúa. Desafortunadamente, el antiguo segmento $SN = 1$ hace una aparición tardía y es aceptado por B antes de que el nuevo segmento $SN = 1$ llegue. Cuando el nuevo segmento $SN = 1$ llega, se le trata como un duplicado y se descarta.

Debe quedar claro que la aparición a destiempo de un segmento antiguo no habría causado dificultades si los números de secuencia no se hubieran solapado. El problema se formula así: ¿qué tamaño debe tener el espacio de secuencia? Esto depende, entre otras cosas, de si la red fuerza un tiempo de vida máximo del paquete y de la tasa a la cual los segmentos se transmiten. Afortunadamente, cada incorporación de un único bit al campo de números de secuencia dobla el espacio de secuencias, de forma que es fácil seleccionar un tamaño seguro.

Control de flujo

El mecanismo de control de flujo por medio de la asignación de créditos descrito anteriormente es bastante robusto en presencia de un servicio de red no fiable y requiere pocas mejoras. Como se ha mencionado, un segmento que contenga ($AN = i$, $W = j$) confirma todos los octetos con números de secuencia inferiores a i y concede créditos para j octetos adicionales comenzando por el octeto i. El mecanismo de asignación de créditos es bastante flexible. Por ejemplo, considere que el último octeto de datos recibido por B fue el octeto número $i - 1$ y que el último segmento enviado por B fue ($AN = i$, $W = j$). Entonces:

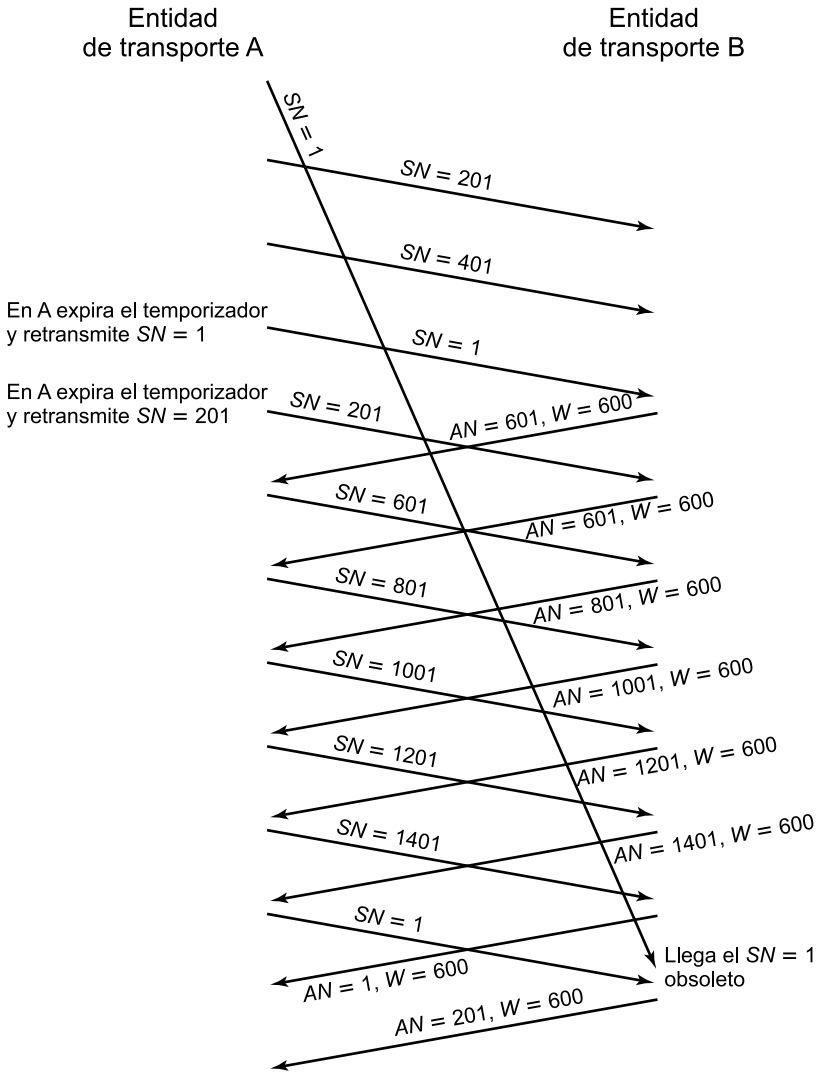

Entidad
de transporte A
Entidad
de transporte B
SN = 1
SN = 201
SN = 401
En A expira el temporizador
y retransmite SN = 1
SN = 1
En A expira el temporizador
y retransmite SN = 201
SN = 201
AN = 601, W = 600
SN = 601
AN = 601, W = 600
SN = 801
AN = 801, W = 600
SN = 1001
AN = 1001, W = 600
SN = 1201
AN = 1201, W = 600
SN = 1401
AN = 1401, W = 600
SN = 1
Llega el SN = 1
obsoleto
AN = 1, W = 600
AN = 201, W = 600

Figura 20.5. Ejemplo de detección incorrecta de duplicado.

- Para incrementar o disminuir los créditos a una cantidad k ($k > j$) cuando no han llegado datos adicionales, B emite ($AN = i$, $W = k$).
- Para confirmar un segmento recibido que contenga m octetos de datos ($m < j$) sin conceder créditos adicionales, B emite ($AN = i + m$, $W = j - m$).

La pérdida de un segmento ACK/CREDIT tiene poco impacto en el funcionamiento del esquema. Confirmaciones posteriores sincronizarán de nuevo el protocolo. Además, si no hay nuevas confirmaciones en camino, en el emisor expirará un temporizador y retransmitirá un segmento de datos, el cual disparará una nueva confirmación. Sin embargo, es aún posible que ocurra un bloqueo mutuo. Considere la situación en la cual B envía ($AN = i$, $W = 0$), cerrando temporalmente la ventana. Con posterioridad, B envía ($AN = i$, $W = j$), pero este segmento se pierde. A está esperando la oportunidad de enviar datos y B piensa que ha concedido esa oportunidad. Para resolver este

problema se puede utilizar un temporizador de ventana. Este temporizador se reinicia cada vez que se envía un segmento (todos los segmentos contienen los campos *AN* y *W*). Si el temporizador expira alguna vez, se le requiere a la entidad de transporte que envíe un segmento, incluso si el nuevo duplica uno anterior. Esto rompe el bloqueo mutuo y le asegura al otro extremo que la entidad de transporte está todavía activo.

Establecimiento de la conexión

Como con otros mecanismos de protocolo, el establecimiento de la conexión debe tener en cuenta la falta de fiabilidad de un servicio de red. Recuérdese que el establecimiento de la conexión requiere el intercambio de SYN, un procedimiento llamado a veces *diálogo en dos pasos*. Supongamos que A emite un SYN a B. Él espera un SYN de vuelta, confirmando la conexión. Dos cosas pueden ir mal: que se pierdan el SYN de A o la respuesta de B. Ambos casos se pueden gestionar mediante el uso de un temporizador de retransmisión de SYN (*véase* Tabla 20.1). A volverá a emitir un SYN cuando el temporizador expire.

Potencialmente, esto puede ocasionar la duplicación de SYN. Si se perdiera el SYN inicial de A, no habría duplicados. Si se perdiera la respuesta de B, entonces B podría recibir dos SYN de A. Es más, si la respuesta de B no se perdiera, sino que simplemente se retrasara, A podría recibir dos SYN de respuesta. Todo esto significa que A y B deben simplemente ignorar los SYN duplicados una vez que la conexión se haya establecido.

Existen otros problemas a los que enfrentarse. Al igual que un SYN retrasado o una respuesta perdida puede producir un SYN duplicado, un segmento de datos retrasado o una confirmación perdida puede dar lugar a la duplicidad de segmentos de datos, como hemos visto en la Figura 20.5. Estos segmentos retrasados o duplicados pueden interferir con la transferencia de datos, tal y como se ilustra en la Figura 20.6. Suponga que con cada nueva conexión, cada entidad del protocolo de transporte inicia la numeración de sus segmentos de datos con el número de secuencia 1. En la figura, una copia duplicada del segmento $SN = 401$ de una antigua conexión llega durante el tiempo de vida de una nueva conexión y se le entrega a la entidad B antes que el segmento de datos legítimo número $SN = 401$. Una forma de abordar este problema es empezar cada nueva conexión con un número de secuencia diferente que difiera lo suficiente del último número de secuencia de la conexión más reciente. Por este motivo, la solicitud de conexión es de la forma SYN *i*, donde *i* es el número de secuencia del primer segmento de datos que será enviado en esta conexión.

Ahora consideremos que un SYN *i* duplicado sobrevive hasta después del cierre de la conexión. La Figura 20.7 representa el problema que puede plantearse. Un SYN *i* obsoleto llega a B después de que la conexión haya terminado. B supone que ésta es una petición nueva y responde con SYN *j*, lo que significa que B acepta la solicitud de conexión y que comenzará a transmitir con $SN = j$. Mientras tanto, A ha decidido abrir una nueva conexión con B y envía SYN *k*. B descarta este último como uno duplicado. Ahora ambos extremos han transmitido y posteriormente recibido un segmento SYN y, por tanto, piensan que existe una conexión válida. Sin embargo, cuando A inicia la transferencia de datos con un segmento numerado con *k*, B rechaza el segmento por no corresponder con la secuencia.

La solución a este problema consiste en que cada lado confirme explícitamente el SYN y número de secuencia del otro. El procedimiento es conocido como *diálogo en tres pasos*. El diagrama de estados de conexión revisado, que es el empleado por TCP, se muestra en la parte superior de la Figura 20.8. Se ha incluido un nuevo estado (*SYN RECEIVED*, «RECIBIDO SYN»). En este

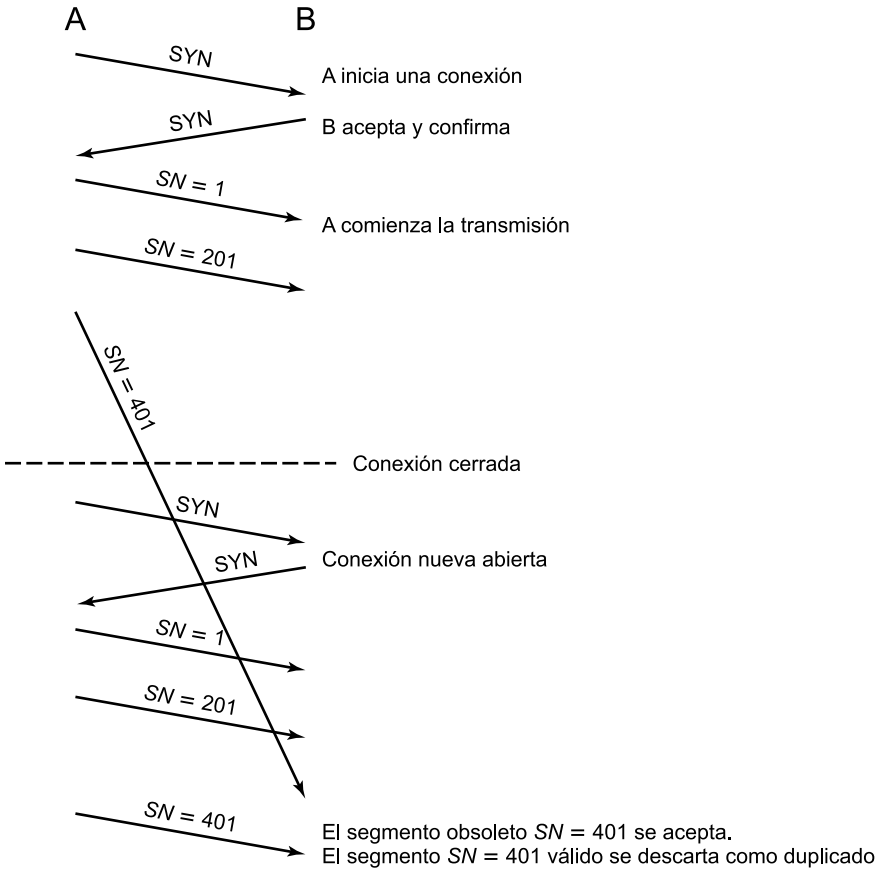


Figura 20.6. Diálogo en dos pasos: problema con un segmento de datos obsoleto.

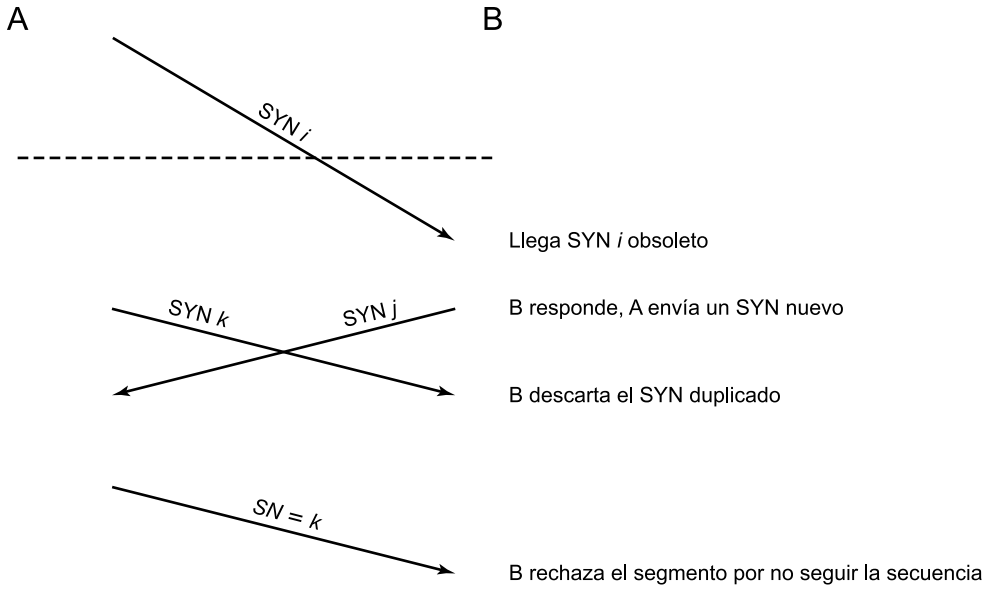


Figura 20.7. Diálogo en dos pasos: problema con segmentos SYN obsoletos.

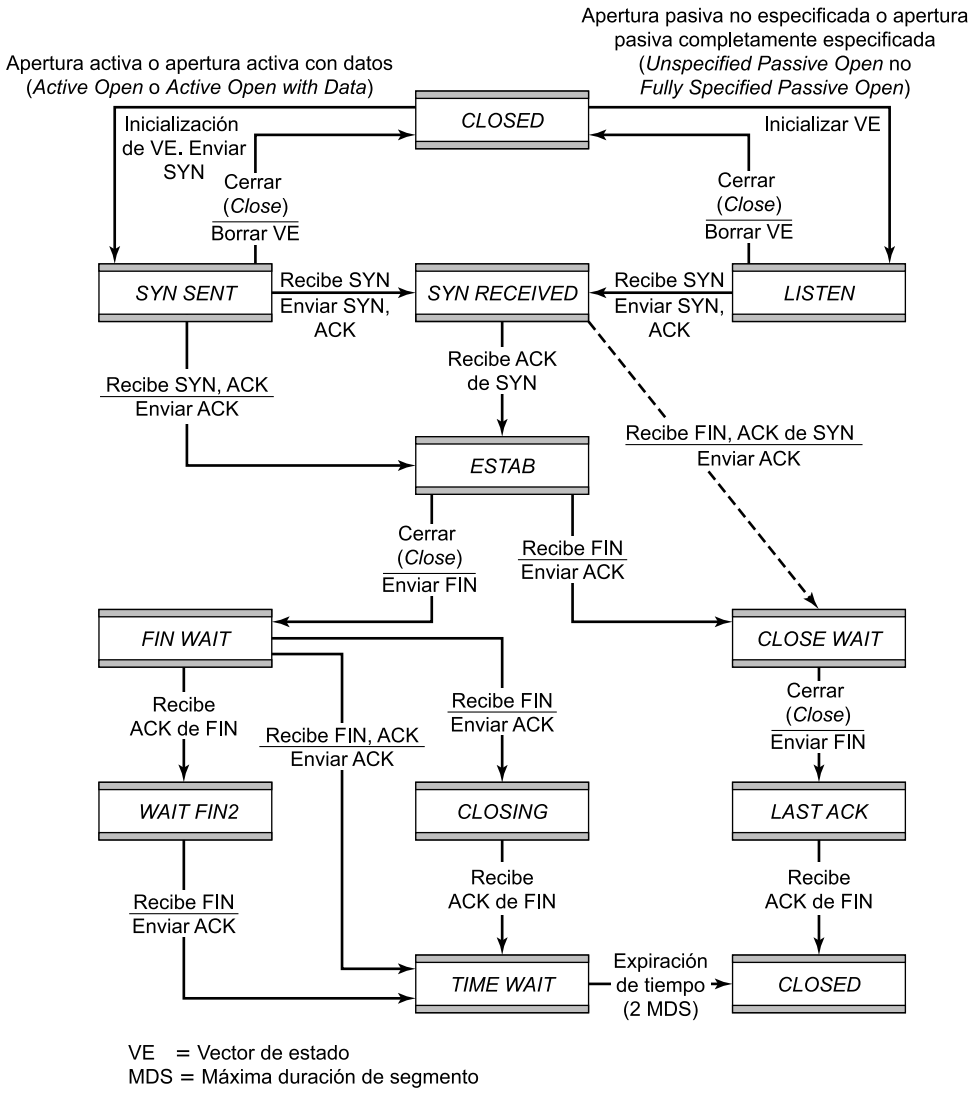

Apertura pasiva no especificada o apertura pasiva completamente especificada (*Unspecified Passive Open* no *Fully Specified Passive Open*)
Apertura activa o apertura activa con datos (*Active Open* o *Active Open with Data*)
CLOSED
Inicialización de VE. Enviar SYN
Cerrar (*Close*) / Borrar VE
Inicializar VE
Cerrar (*Close*) / Borrar VE
SYN SENT
Recibe SYN / Enviar SYN, ACK
SYN RECEIVED
Recibe SYN / Enviar SYN, ACK
LISTEN
Recibe SYN, ACK / Enviar ACK
Recibe ACK de SYN
Recibe FIN, ACK de SYN / Enviar ACK
ESTAB
Cerrar (*Close*) / Enviar FIN
Recibe FIN / Enviar ACK
FIN WAIT
CLOSE WAIT
Recibe ACK de FIN
Recibe FIN, ACK / Enviar ACK
Recibe FIN / Enviar ACK
Cerrar (*Close*) / Enviar FIN
WAIT FIN2
CLOSING
LAST ACK
Recibe FIN / Enviar ACK
Recibe ACK de FIN
Recibe ACK de FIN
TIME WAIT
Expiración de tiempo (2 MDS)
CLOSED
VE = Vector de estado
MDS = Máxima duración de segmento

Figura 20.8. Diagrama de estados de la entidad TCP.

estado, la entidad de transporte procede cautelosamente durante el proceso de apertura de la conexión para asegurar que los segmentos SYN enviados por las dos partes han sido confirmados antes de que se declare establecida la conexión. Además del nuevo estado, hay un nuevo segmento de control (RST) para reiniciar el otro lado cuando se detecte un SYN duplicado.

La Figura 20.9 ilustra el funcionamiento típico del diálogo en tres pasos. En la Figura 20.9a, la entidad de transporte A inicia la conexión con un SYN que incluye el número de secuencia de envío, *i*. El valor *i* es el número de secuencia inicial (ISN) y se asocia con el SYN. El primer octeto de datos a transmitir tendrá el número de secuencia $i + 1$. El SYN de respuesta confirma el ISN con ($AN = i + 1$) e incluye su propio ISN. A confirma el SYN/ACK de B en su primer segmento de datos, que comienza con el número de secuencia $i + 1$. La Figura 20.9b muestra una situación en la cual un SYN *i* obsoleto llega a B tras el cierre de la conexión pertinente. B supone que es una solicitud nueva y responde con SYN *j*, $AN = i + 1$. Cuando A recibe este mensaje, se

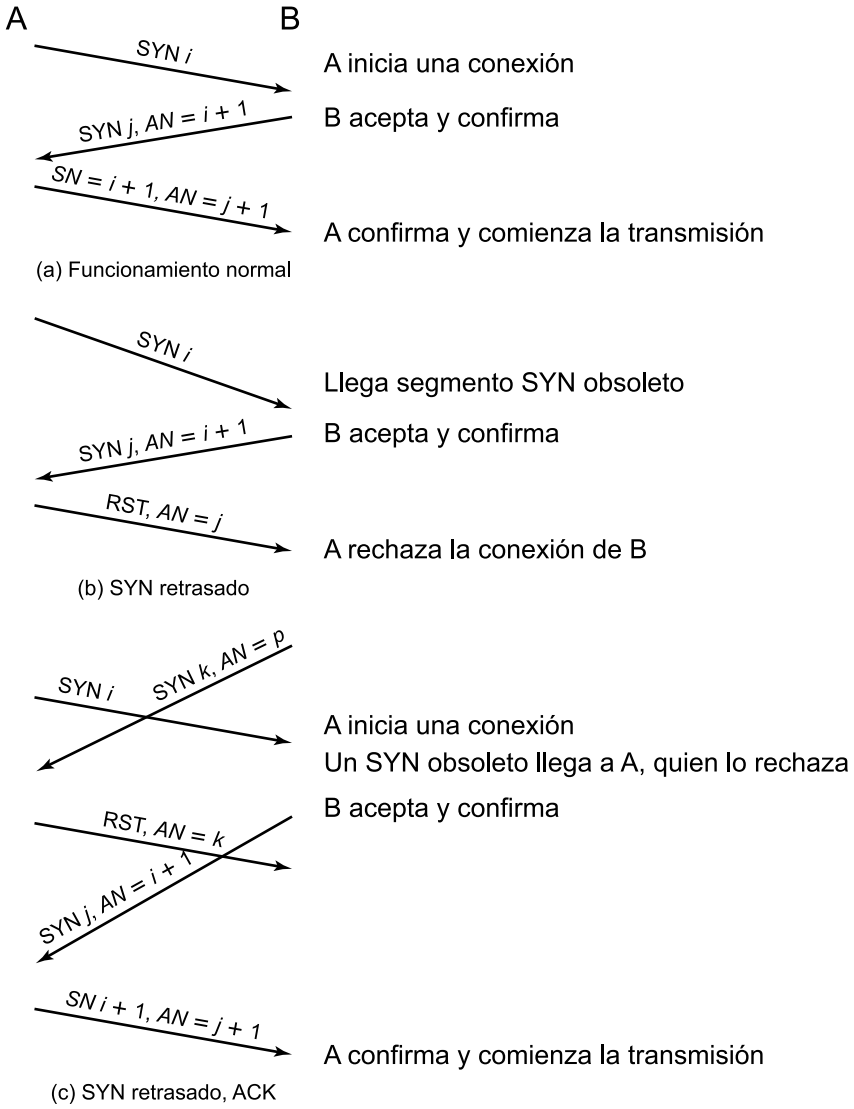

A
B
SYN i
A inicia una conexión
SYN j, AN = i + 1
B acepta y confirma
SN = i + 1, AN = j + 1
A confirma y comienza la transmisión
(a) Funcionamiento normal
SYN i
Llega segmento SYN obsoleto
SYN j, AN = i + 1
B acepta y confirma
RST, AN = j
A rechaza la conexión de B
(b) SYN retrasado
SYN i
SYN k, AN = p
A inicia una conexión
Un SYN obsoleto llega a A, quien lo rechaza
B acepta y confirma
RST, AN = k
SYN j, AN = i + 1
SN i + 1, AN = j + 1
A confirma y comienza la transmisión
(c) SYN retrasado, ACK

Figura 20.9. Ejemplos de diálogo en tres pasos.

da cuenta de que él no ha solicitado una conexión y, por tanto, envía un RST, $AN = j$. Observe que la porción $AN = j$ del mensaje RST es esencial para que un RST duplicado obsoleto no cancele un establecimiento de conexión legítimo. La Figura 20.9c muestra un caso en que un SYN/ACK antiguo llega en mitad del establecimiento de una nueva conexión. Debido al uso de números de secuencia en las confirmaciones, este evento no causa perjuicio alguno.

Por simplicidad, la parte superior de la Figura 20.8 no incluye transiciones en las que se envíe un segmento RST. La regla básica consiste en enviar un RST si el estado de la conexión no es todavía ESTAB y se recibe un ACK inválido (uno que no referencie a algún segmento que haya sido enviado). El lector debe probar varias combinaciones de eventos para ver que este procedimiento de establecimiento de conexión funciona ante cualquier combinación de segmentos obsoletos o perdidos.

Cierre de la conexión

El diagrama de estados de la Figura 20.3 define el uso de un simple diálogo en dos pasos para el establecimiento de la conexión, que ha resultado ser insatisfactorio para el caso de un servicio de red no fiable. De igual forma, el diálogo en dos pasos definido en ese diagrama para el cierre de la conexión es inadecuado para un servicio de red no fiable. El siguiente escenario podría darse por la llegada de los segmentos en desorden. Una entidad de transporte en el estado *CLOSE WAIT* envía su último segmento de datos, seguido por un segmento FIN, pero el segmento FIN llega al otro extremo antes que el último segmento de datos. La entidad de transporte receptora aceptará ese FIN, cerrará la conexión y perderá el último segmento de datos. Para evitar este problema se puede asociar al segmento FIN un número de secuencia, que puede ser el siguiente número de secuencia tras el último octeto de los datos transmitidos. Con este refinamiento, la entidad de transporte receptora, después de recibir un FIN, antes de cerrar la conexión esperará si es necesario a los datos que lleguen tarde.

Un problema más serio lo constituye la potencial pérdida de segmentos y la posible presencia de segmentos obsoletos. La Figura 20.8 muestra que el procedimiento de cierre adopta una solución similar a la usada para el establecimiento de la conexión. Cada extremo debe explícitamente confirmar el segmento FIN del otro usando un ACK con número de secuencia del FIN a confirmar. Para realizar un cierre ordenado, una entidad de transporte requiere lo siguiente:

- Debe enviar un FIN i y recibir un $AN = i + 1$.
- Debe recibir un FIN j y enviar un $AN = j + 1$.
- Debe esperar un intervalo de tiempo igual a dos veces el máximo tiempo de vida esperado de un segmento.

Recuperación de interrupciones

Cuando el sistema sobre el cual una entidad de transporte se está ejecutando falla y posteriormente se recupera, la información de estado de todas las conexiones activas se pierde. Las conexiones afectadas pasan a estar «semiabiertas» ya que el lado que no se vio afectado por la interrupción no se ha dado cuenta todavía del problema.

El extremo todavía activo de la conexión semiabierta puede cerrar la conexión usando un temporizador de persistencia. Este temporizador mide el tiempo que la máquina de transporte continuará esperando una confirmación (u otra respuesta apropiada) de un segmento transmitido después de que el segmento haya sido retransmitido el máximo número de veces. Cuando el temporizador expira, la entidad de transporte asume que ha fallado la otra entidad o la red intermedia, cierra la conexión e indica al usuario TS que se produjo un cierre anormal.

En el caso en que una entidad de transporte falle y se reinicie rápidamente, la conexión semiabierta se puede terminar más rápidamente mediante el uso del segmento RST. El lado que falla devuelve un RST i por cada segmento i que reciba. Cuando el RST i se recibe en el otro extremo, se debe comprobar su validez basándose en el número de secuencia i, ya que el RST podría ser la respuesta a un segmento obsoleto. Si el reinicio es válido, la entidad de transporte efectúa un cierre anormal.

Estas medidas solucionan la situación en la capa de transporte. La decisión de reabrir la conexión se deja a los usuarios TS. El problema es de sincronización. Cuando ocurrió la interrupción, puede que hubiera uno o más segmentos pendientes en ambos sentidos. El usuario del TS del lado

que no falló sabe cuántos datos ha recibido, pero el otro usuario puede que no, si la información de estado se hubiera perdido. Así, existe el peligro de que algunos datos de usuario se pierdan o se dupliquen.

20.2. TCP

En esta sección examinaremos TCP (RFC 793). En primer lugar, analizaremos el servicio que ofrece al usuario de TS y luego los detalles internos del protocolo.

SERVICIOS TCP

TCP está diseñado para proporcionar una comunicación fiable entre pares de procesos (usuarios TCP) a través de una gran variedad de redes e interconexiones fiables y no fiables. TCP proporciona dos servicios útiles para etiquetar los datos: forzado y urgente:

- **Flujo de datos forzado.** Normalmente, TCP decide cuándo se han acumulado suficientes datos para formar un segmento para su transmisión. El usuario TCP puede requerir que TCP transmita todos los datos pendientes, a los que incluye una etiqueta con un indicador de forzado. En el extremo receptor, TCP entregará los datos al usuario en la misma forma. Un usuario podría requerir esto si se detecta a una interrupción lógica en los datos.
- **Señalización de datos urgentes.** Proporciona un medio para informar al usuario TCP destino que en el flujo de datos que recibe existen datos significativos o «urgentes». Es responsabilidad del usuario destino determinar la acción apropiada.

Como en IP, los servicios proporcionados por TCP se definen en términos de primitivas y parámetros. Los servicios proporcionados por TCP son considerablemente más ricos que los proporcionados por IP y, por tanto, el conjunto de primitivas y parámetros es más complejo. La Tabla 20.2 enumera las primitivas de solicitud de servicio TCP, que son emitidas por un usuario TCP a TCP, y la Tabla 20.3 enumera las primitivas de respuesta de servicio TCP, emitidas por TCP a un usuario TCP local. La Tabla 20.4 proporciona una breve definición de los parámetros involucrados. Las dos órdenes de apertura pasiva indican el deseo del usuario TCP de aceptar una petición de conexión. La apertura activa con datos permite al usuario comenzar transmitiendo datos en la apertura de la conexión.

FORMATO DE LA CABECERA TCP

TCP utiliza un único tipo de unidad de datos de protocolo, llamado segmento TCP. La cabecera se muestra en la Figura 20.10. Ya que una cabecera debe servir para llevar a cabo todos los mecanismos del protocolo, ésta es más bien grande, con una longitud mínima de 20 octetos. Sus campos son los siguientes:

- **Puerto origen (16 bits):** usuario TCP origen.
- **Puerto destino (16 bits):** usuario TCP destino.
- **Número de secuencia (32 bits):** número de secuencia del primer octeto de datos en este segmento, excepto cuando está presente el indicador SYN. Si el indicador SYN está activo, se trata del número de secuencia inicial (ISN) y el primer octeto de datos es el ISN + 1.

Tabla 20.2. Primitivas de solicitud de servicio TCP.

Primitiva	Parámetros	Descripción
Apertura pasiva no especificada *(Unspecified Passive Open)*	puerto origen, [tiempo de expiración], [acción tras expiración], [precedencia], [rango de seguridad]	Preparado para intentos de conexión desde cualquier destino remoto, con una seguridad y precedencia especificadas.
Apertura pasiva completamente especificada *(Fully Specified Passive Open)*	puerto origen, puerto destino, dirección-destino, [tiempo de expiración], [acción tras expiración], [precedencia], [rango de seguridad]	Preparado para intentos de conexión desde destino remoto especificado con una seguridad y precedencia especificadas.
Apertura activa *(Active Open)*	puerto origen, puerto destino, dirección destino, [tiempo de expiración], [acción tras expiración], [precedencia], [seguridad]	Solicita una conexión a un destino especificado, con una seguridad y precedencia particulares.
Apertura activa con datos *(Active Open with Data)*	puerto origen, puerto destino, dirección destino, [tiempo de expiración], [acción tras expiración], [precedencia], [seguridad], datos, longitud de datos, indicador FORZADO, indicador URGENTE	Solicita una conexión a un destino especificado, con una seguridad y precedencia particulares, transmitiendo datos con la solicitud.
Enviar *(Send)*	nombre de conexión local, datos, longitud de datos, indicador FORZADO, indicador URGENTE, [tiempo de expiración], [acción tras expiración]	Transfiere datos a través de la conexión indicada.
Asignar *(Allocate)*	nombre de conexión local, longitud de datos	Expide un incremento en la asignación de créditos para la recepción de datos en TCP.
Cerrar *(Close)*	nombre de conexión local	Efectúa un cierre ordenado de la conexión
Abortar *(Abort)*	nombre de conexión local	Efectúa un cierre abrupto de la conexión
Estado *(Status)*	nombre de conexión local	Consulta el estado de la conexión

Nota: los corchetes indican parámetros opcionales.

- **Número de confirmación (32 bits):** contiene el número de secuencia del siguiente octeto que la entidad TCP espera recibir.
- **Longitud de la cabecera (4 bits):** número de palabras de 32 bits de la cabecera.
- **Reservado (6 bits):** bits reservados para uso futuro. El RFC 3168 usa dos de esos bits para la función de notificación explícita de congestión. Una discusión sobre esta función está fuera de nuestro alcance.
- **Indicadores (6 bits):**

  URG: el campo de puntero urgente es válido.

  ACK: el campo de confirmación es válido.

  PSH: función de forzado.

Tabla 20.3. Primitivas de respuesta del servicio TCP.

Primitiva	Parámetros	Descripción
Identificador de apertura *(Open ID)*	nombre de conexión local, puerto origen, puerto destino*, dirección destino*	Informa al usuario TCP del nombre de conexión asignado a la conexión pendiente solicitada mediante una primitiva de apertura.
Apertura fallida *(Open Failure)*	nombre de conexión local	Informa sobre un fallo de una solicitud de apertura activa.
Apertura correcta *(Open Success)*	nombre de conexión local	Informa sobre la conclusión de una solicitud apertura pendiente.
Entrega *(Deliver)*	nombre de conexión local, datos, longitud de datos, indicador URGENTE	Informa sobre la llegada de datos.
Cierre *(Closing)*	nombre de conexión local	Informa que el usuario TCP remoto ha emitido una orden «cerrar» y que todos los datos enviados por el mismo han sido entregados.
Terminación *(Terminate)*	nombre de conexión local, descripción	Informa que la conexión se ha terminado. Se proporciona una descripción de la razón por la que ha finalizado.
Respuesta de estado *(Status Response)*	nombre de conexión local, puerto origen, puerto destino, dirección origen, dirección destino, ventana de recepción, ventana de envío, cantidad que espera ACK, cantidad por recibir, estado urgente, precedencia, seguridad, tiempo de expiración	Informa del estado actual de la conexión.
Error *(Error)*	nombre de conexión local, descripción	Notifica errores internos o referentes a la solicitud de un servicio.

* = No empleado en la apertura pasiva no especificada.

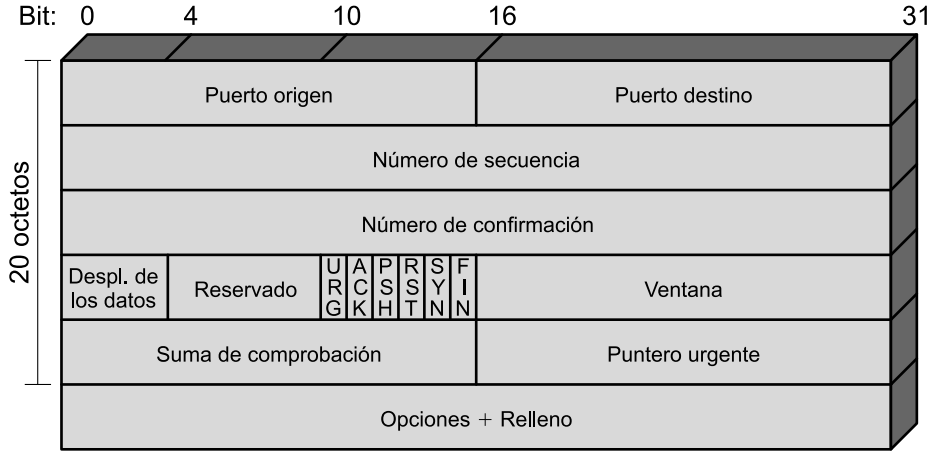


Figura 20.10. Cabecera de TCP.

Tabla 20.4. Parámetros de servicio TCP.

Puerto origen	Usuario TCP local.
Tiempo expiración	El mayor retardo permitido para la entrega de datos antes de efectuar un cierre automático de la conexión o de generar un informe de error. Especificado por el usuario.
Acción tras expiración	Indica qué hacer en caso de expiración de tiempo: terminar la conexión o notificar un error al usuario TCP.
Precedencia	Nivel de precedencia para una conexión. Toma valores de cero (el más bajo) a siete (más alto). Es el mismo parámetro que en IP.
Rango de seguridad	Rangos permitidos en compartimiento, restricciones en la gestión, códigos de control de transmisión y niveles de seguridad.
Puerto destino	Usuario TCP remoto.
Dirección destino	Dirección Internet del computador remoto.
Seguridad	Información de seguridad de una conexión, incluyendo el nivel de seguridad, compartimiento, restricciones en la gestión y códigos de control de transmisión. Son los mismos parámetros que en IP.
Datos	Bloque de datos enviado por el usuario TCP o entregado a un usuario TCP.
Longitud datos	Longitud de los datos enviados o entregados.
Indicador FORZADO (PSH)	Si está activado indica que a los datos asociados se les debe proporcionar el servicio de flujo de datos forzado.
Indicador URGENTE (URG)	Si está activado indica que a los datos asociados se les debe proporcionar el servicio de señalización de datos urgentes.
Nombre de conexión local	Identificador de una conexión definida por un par del tipo (socket local, socket remoto). Lo proporciona TCP.
Descripción	Información suplementaria en una primitiva *Terminate* o *Error.*
Dirección fuente	Dirección Internet del computador local.
Estado de la conexión	Estado de la conexión referenciada (CLOSED, ACTIVE OPEN, PASSIVE OPEN, ESTAB, CLOSING).
Ventana de recepción	Cantidad de datos, en octetos, que la entidad TCP local está dispuesta a recibir.
Ventana de envío	Cantidad de datos, en octetos, que se permite enviar a la entidad TCP remota.
Cantidad que espera ACK	Cantidad de datos previamente transmitidos que esperan confirmación.
Cantidad por recibir	Cantidad de datos, en octetos, almacenados temporalmente en la entidad TCP local, pendientes de ser recibidos por el usuario TCP local.
Estado urgente	Informa al usuario TCP que recibe datos de si hay datos urgentes disponibles o de si todos los datos urgentes, en caso de que hubieran, han sido entregados al usuario.

RST: reiniciar la conexión.

SYN: sincronizar los números de secuencia.

FIN: el emisor no enviará más datos.

- **Ventana (16 bits):** asignación de créditos para el control de flujo, en octetos. Contiene el número de octetos de datos, comenzando con el número de secuencia que se indica en el campo de confirmación que el emisor está dispuesto a aceptar.

- **Suma de comprobación (16 bits):** el complemento a uno de la suma modular complemento a uno de todas las palabras de 16 bits del segmento más una pseudocabecera, descrita más adelante[2].
- **Puntero urgente (16 bits):** este valor, cuando se suma al número de secuencia del segmento, contiene el número de secuencia del último octeto de la secuencia de datos urgentes. Esto permite al receptor conocer la cantidad de datos urgentes que llegan.
- **Opciones (Variable):** un ejemplo lo constituye la opción que especifica la longitud máxima de segmento que será aceptada.

El *número de secuencia* y el *número de confirmación* hacen referencia a octetos en lugar de a segmentos completos. Por ejemplo, si un segmento contiene el número de secuencia 1001 e incluye 600 octetos de datos, el número de secuencia se refiere al primer octeto del campo de datos. El segmento siguiente en orden lógico tendrá el número de secuencia 1601. De esta manera, TCP está lógicamente orientado a flujo: acepta un flujo de octetos del usuario, los agrupa en segmentos según vea apropiado y numera cada octeto del flujo.

El campo *suma de comprobación* se aplica a todo el segmento más una pseudocabecera incorporada en el momento del cálculo (tanto en la transmisión como en la recepción). La pseudocabecera incluye los siguientes campos de la cabecera IP: dirección red origen y destino, el protocolo y un campo de longitud del segmento. Con la inclusión de la pseudocabecera, TCP se protege ante un reparto erróneo de IP. Es decir, si IP entrega un segmento a una estación errónea, aunque el segmento esté libre de errores de bits, la entidad TCP receptora detectará el error del entrega.

Comparando la cabecera TCP con la interfaz de usuario TCP definida en las Tablas 20.2 y 20.3, el lector podría pensar que faltan algunos campos en la cabecera TCP. Éste es efectivamente el caso. TCP está diseñado específicamente para trabajar con IP. Por tanto, algunos parámetros de usuario se pasan a través de TCP a IP para su inclusión en la cabecera IP. Los más relevantes son:

- Precedencia: un campo de 3 bits.
- Retardo-normal/bajo-retardo.
- Rendimiento-normal/alto-rendimiento.
- Fiabilidad-normal/alta-fiabilidad.
- Seguridad: un campo de 11 bits.

Merece la pena observar que este vínculo TCP/IP significa que la sobrecarga mínima requerida para cada unidad de datos es, en realidad, de 40 octetos.

MECANISMOS TCP

Podemos agrupar los mecanismos de TCP en las categorías de establecimiento de la conexión, transferencia de datos y cierre de la conexión.

Establecimiento de la conexión

El establecimiento de la conexión en TCP siempre utiliza un diálogo en tres pasos. Cuando el indicador SYN está activado, el segmento es esencialmente una solicitud de conexión y funciona tal y

[2] Se puede encontrar una discusión sobre esta suma de comprobación en un documento de apoyo en la página web de este libro.

como se explicó en la Sección 20.1. Para iniciar una conexión, una entidad envía un SYN, $SN = X$, donde X es el número de secuencia inicial. El receptor responde con SYN, $SN = Y$, $AN = X + 1$ mediante la activación de los indicadores SYN y ACK. Observe que la confirmación indica que el receptor está ahora esperando recibir un segmento que comience con el octeto de datos $X + 1$, confirmando el SYN que ocupaba $SN = X$. Finalmente, el que inicia la conexión responde con $AN = Y + 1$. Si los dos extremos emiten SYN cruzados, no se produce ningún problema: ambos lados responden con SYN/ACK (*véase* Figura 20.4).

Una conexión está únivocamente determinada por los sockets (estación, puerto) origen y destino. Así, en cualquier instante de tiempo, sólo puede haber una única conexión TCP entre un único par de puertos. Sin embargo, un puerto dado puede admitir múltiples conexiones, cada una con un puerto diferente.

Transferencia de datos

Aunque los datos se transmiten en segmentos sobre una conexión de transporte, la transferencia de datos se ve desde un punto de vista lógico como un flujo de octetos. Por tanto, cada octeto es numerado módulo 2^{32}. Cada segmento contiene el número de secuencia del primer octeto del campo de datos. El control de flujo se ejerce utilizando un esquema de asignación de créditos, en el cual el crédito es un número de octetos en lugar de un número de segmentos, tal y como se explicó en la Sección 20.1.

La entidad de transporte almacena temporalmente los datos tanto en la transmisión como en la recepción. TCP normalmente aplica su propio criterio para decidir cuándo construir un segmento para transmitirlo y cuándo entregar los datos recibidos al usuario. El indicador *PUSH* («FORZADO») se usa para obligar a que los datos acumulados sean enviados por el transmisor y entregados al usuario por el receptor. Esto sirve como una función de fin de bloque.

El usuario puede especificar que un bloque de datos es urgente. TCP designará el fin de ese bloque con un puntero de urgente y lo enviará en el flujo de datos ordinario. El usuario receptor es alertado de que se están recibiendo datos urgentes.

Si durante el intercambio de datos llega un segmento que aparentemente no va dirigido a la conexión actual, se envía un segmento con el valor del indicador RST activado. Los SYN duplicados retrasados y las confirmaciones de datos todavía no enviados constituyen ejemplos de esta situación.

Cierre de la conexión

El procedimiento normal de finalización de una conexión es un cierre ordenado. Cada usuario TCP debe emitir una primitiva *Close*. La entidad de transporte establece el bit FIN en el último segmento que envía y que contiene los últimos datos a enviar sobre esa conexión.

Si el usuario emite una primitiva *Abort* («abortar») se produce un cierre abrupto. En este caso, la entidad de transporte abandona todos los intentos de enviar o recibir datos y descarta los datos de sus memorias temporales de transmisión y recepción. Se envía un segmento RST al otro extremo.

OPCIONES EN LOS CRITERIOS DE IMPLEMENTACIÓN DE TCP

El estándar TCP proporciona una especificación precisa del protocolo que se va a utilizar entre entidades TCP. Sin embargo, ciertos aspectos del protocolo admiten varias opciones de implementación posibles. Aunque dos implementaciones que escojan opciones alternativas pueden interoperar, puede haber consecuencias en el rendimiento. Las áreas de diseño para las que se especifican opciones son las siguientes:

- Política de envío.
- Política de entrega.
- Política de aceptación.
- Política de retransmisión.
- Política de confirmación.

Política de envío

En ausencia de datos marcados con el indicador de forzado y de una ventana de transmisión cerrada (*véase* Figura 20.2a), una entidad TCP emisora es libre de enviar los datos tan pronto como le sea posible, dentro de su asignación actual de crédito. Conforme los datos son emitidos por el usuario se almacenan en la memoria temporal de transmisión. TCP puede construir un segmento por cada lote de datos proporcionado por su usuario o puede esperar a que se acumule una cierta cantidad de datos antes de construir y enviar el segmento. La política concreta dependerá de consideraciones sobre el rendimiento. Si las transmisiones son largas e infrecuentes, hay poca sobrecarga en términos de generación y procesamiento de segmentos. Por otro lado, si las transmisiones son frecuentes y pequeñas, entonces el sistema está proporcionando una respuesta rápida.

Política de entrega

En ausencia del indicador de forzado, una entidad TCP receptora es libre de entregar los datos al usuario tan pronto como le sea posible. Puede entregar los datos conforme se reciben los segmentos en orden, o puede almacenar los datos de varios segmentos en las memorias temporales de recepción antes de efectuar la entrega. La política concreta dependerá de consideraciones sobre el rendimiento. Si las entregas son infrecuentes y voluminosas, el usuario no recibe los datos tan pronto como puede ser deseable. Por otro lado, si las entregas son frecuentes y pequeñas, puede haber un procesamiento innecesario en TCP y en el software del usuario, así como un número innecesario de interrupciones del sistema operativo.

Política de aceptación

Cuando todos los segmentos de datos llegan en orden sobre una conexión TCP, TCP coloca los datos en una memoria temporal de recepción para entregarlos al usuario. Es posible, sin embargo, que los segmentos no lleguen en secuencia. En este caso, la entidad TCP receptora tiene dos opciones:

- Aceptación **ordenada:** acepta sólo segmentos que llegan en orden. Todos los segmentos que no lleguen en secuencia se descartan.
- Aceptación **en ventana:** acepta todos los segmentos que estén dentro de la ventana de recepción (*véase* Figura 20.2b).

La política de aceptación ordenada da lugar a una implementación sencilla, pero sitúa una carga adicional sobre el servicio de red, ya que la entidad TCP que envía debe retransmitir, tras la expiración de los temporizadores correspondientes, aquellos segmentos que se recibieron correctamente pero que fueron descartados por su recepción desordenada. Además, si se pierde un único segmento en el camino, entonces deben retransmitirse todos los segmentos siguientes una vez que expire en el TCP emisor el temporizador del segmento perdido.

La política de aceptación en ventana puede reducir las transmisiones, pero requiere una comprobación de aceptación más compleja y un esquema de almacenamiento de datos más sofisticado para almacenar y llevar el registro de los datos desordenados aceptados.

Política de retransmisión

TCP mantiene una cola de los segmentos que han sido enviados pero que todavía no han sido confirmados. La especificación de TCP establece que TCP retransmite un segmento si no recibe una confirmación dentro de un tiempo determinado. Una implementación de TCP puede emplear una de estas tres estrategias de retransmisión:

- **Sólo el primero:** mantiene un temporizador de retransmisión para toda la cola. Si se recibe una confirmación, elimina de la cola el segmento o segmentos correspondientes y reinicia el temporizador. Si el temporizador expira, retransmite el primer segmento de la cola y reinicia el temporizador.
- **Por lotes:** mantiene un temporizador de retransmisión para toda la cola. Si se recibe una confirmación, elimina de la cola el segmento o segmentos correspondientes y reinicia el temporizador. Si el temporizador expira, retransmite todos los segmentos de la cola y reinicia el temporizador.
- **Individual:** mantiene un temporizador de retransmisión por cada segmento en cola. Si se recibe una confirmación, elimina de la cola el segmento o segmentos apropiados y destruye el temporizador o los temporizadores asociados. Si algún temporizador expira, retransmite el segmento correspondiente y reinicia temporizador.

La política de sólo el primero es eficiente en términos de tráfico generado, ya que solamente se retransmiten los segmentos perdidos (o segmentos cuyo ACK se perdió). Ya que el temporizador para el segundo segmento en la cola no se establece hasta que el primer segmento se confirma, pueden producirse retardos considerables. La política de retransmisión individual soluciona este problema a expensas de una implementación más compleja. La política de retransmisión por lotes también reduce la posibilidad de largos retardos, pero puede producir retransmisiones innecesarias. La efectividad real de una política de retransmisión depende en parte de la política de aceptación del receptor. Si el receptor está empleando una política de aceptación ordenada, entonces descartará los segmentos recibidos tras un segmento perdido. Esta política encaja mejor con una retransmisión por lotes. Si el receptor emplea una política de aceptación en ventana, entonces es mejor la política de retransmisión del primero solamente o de retransmisión individual. Por supuesto, en una red mixta de computadores, se pueden usar ambas políticas de aceptación.

Política de confirmación

Cuando llega un segmento en orden, la entidad TCP receptora tiene dos opciones en cuanto a la generación de las confirmaciones:

- **Inmediata:** cuando los datos se aceptan, se transmite inmediatamente un segmento vacío (sin datos) que contiene el número de confirmación apropiado.
- **Acumulada:** cuando se aceptan los datos, se registra la necesidad de una confirmación, pero espera un segmento de datos de salida con datos e incorpora la confirmación. Para evitar grandes retardos, establece un temporizador de ventana (*véase* Tabla 20.1). Si el temporizador expira antes de que se envíe una confirmación, transmite un segmento vacío que contiene el número de confirmación apropiado.

La política de confirmación inmediata es sencilla y mantiene a la entidad TCP remota completamente informada, lo que evita retransmisiones innecesarias. Sin embargo, esta política da lugar a retransmisiones de segmentos extra, a saber, segmentos vacíos usados sólo para confirmar. Además, esta política puede ocasionar una mayor carga en la red. Considere que una entidad TCP recibe un segmento e inmediatamente envía un ACK. Entonces, los datos se pasan a la aplicación, lo cual expande la ventana de recepción, emitiendo otro segmento TCP vacío para proporcionar crédito adicional a la entidad TCP emisora.

A causa de la potencial sobrecarga causada por la política de confirmación inmediata, normalmente se emplea la política de confirmación acumulada. Reconozcamos, sin embargo, que el uso de esta política requiere más procesamiento en el extremo receptor y complica en la entidad TCP emisora la tarea de estimar el retardo de ida y vuelta.

20.3. CONTROL DE CONGESTIÓN DE TCP

El mecanismo de control de flujo basado en créditos de TCP se diseñó para permitir que el destino restrinja el flujo de segmentos de una fuente y evitar así la saturación de la memoria temporal del destino. Este mismo mecanismo de control de flujo se utiliza ahora de varias formas ingeniosas para proporcionar control de congestión sobre Internet entre la fuente y el destino. La congestión, como ya se ha visto varias veces en este libro, tiene dos efectos principales. En primer lugar, cuando la congestión empieza a producirse, el tiempo de transmisión a través de la red o interconexión de redes aumenta. En segundo lugar, conforme la congestión se hace más severa, la red o los nodos de la interconexión descartan paquetes. El mecanismo de control de flujo de TCP se puede utilizar para identificar el comienzo de la congestión (identificando el incremento de los tiempos de retardo y de los segmentos descartados) y reaccionar mediante la reducción del flujo de datos. Si muchas de las entidades TCP que operan a lo largo de una red practican este tipo de control, la congestión de la red se puede aliviar.

Desde la publicación del RFC 793, se han implementado varias técnicas que pretenden mejorar las características de control de congestión de TCP. Ninguna de estas técnicas extienden o violan el estándar TCP original. Más bien representan criterios de implementación que están dentro del ámbito de la especificación de TCP. Muchas de estas técnicas son de uso obligatorio en TCP, como se refleja en el RFC 1122 («Requisitos para las estaciones en Internet»), mientras otras se especifican en el RFC 2581. Las técnicas se pueden agrupar, en un sentido amplio, en dos categorías: gestión de temporizadores de retransmisión y gestión de la ventana. En esta sección se examinan algunas de las técnicas más importantes y más utilizadas.

GESTIÓN DE TEMPORIZADORES DE RETRANSMISIÓN

Conforme cambian las condiciones de red o interconexión de redes, un temporizador de retransmisión estático puede expirar demasiado tarde o demasiado pronto. De acuerdo a esto, virtualmente

todas las implementaciones de TCP intentan estimar el retardo de ida y vuelta actual mediante la observación del patrón del retardo de los segmentos más recientes, para establecer el temporizador a un valor un poco mayor que el retardo de ida y vuelta estimado.

Promediado simple

Una posible opción consistiría en tomar simplemente la media de los tiempos de ida y vuelta observados sobre un determinado número de segmentos. Si la media predice con precisión los retardos de ida y vuelta futuros, entonces el temporizador de retransmisión realizará su función apropiadamente. El método del promediado simple se puede expresar como:

$$\mathrm{ARTT}(K+1) = \frac{1}{K+1}\sum_{i=1}^{K+1}\mathrm{RTT}(i) \tag{20.1}$$

donde RTT(i) es el tiempo de ida y vuelta observado para el segmento i-ésimo transmitido y ARTT(K) es el tiempo de ida y vuelta medio de los K primeros segmentos.

Esta expresión se puede reescribir como:

$$\mathrm{ARTT}(K+1) = \frac{K}{K+1}\,\mathrm{ARTT}(K) + \frac{1}{K+1}\,\mathrm{RTT}(K+1) \tag{20.2}$$

Con esta formulación, no es necesario recalcular la sumatoria completa cada vez.

Promediado exponencial

Observe que a cada término de la sumatoria se le da el mismo peso. Es decir, cada término se multiplica por la misma constante $1/(K+1)$. Normalmente, nos interesaría dar mayor peso a los retardos más recientes, ya que es más probable que reflejen el comportamiento futuro. Una técnica común para predecir los valores siguientes a partir de una serie temporal de valores pasados, y que es el especificado en el RFC 793, es el promediado exponencial:

$$\mathrm{SRTT}(K+1) = \alpha \times \mathrm{SRTT}(K) + (1-\alpha) \times \mathrm{RTT}(K+1) \tag{20.3}$$

donde SRTT(K) se denomina estimación del tiempo de ida y vuelta suavizado y donde se define SRTT(0) = 0. Compárese esta ecuación con la Ecuación (20.2). Mediante el uso de un valor constante de $\alpha (0 < \alpha < 1)$, independientemente del número de observaciones pasadas, tenemos una circunstancia en la cual se consideran todas los valores pasados, pero con menor peso las más distantes. Para ver esto más claramente, consideremos el desarrollo de la Ecuación (20.3):

$$\begin{aligned}\mathrm{SRTT}(K+1) = {} & (1-\alpha)\mathrm{RTT}(K+1) + \alpha(1-\alpha)\mathrm{RTT}(K) + \\ & + \alpha^2(1-\alpha)\mathrm{RTT}(K-1) + \cdots + \alpha^K(1-\alpha)\mathrm{RTT}(1)\end{aligned}$$

Ya que α y $(1-\alpha)$ son menores que uno, cada término sucesivo en la ecuación precedente es menor. Por ejemplo, para $\alpha = 0{,}8$, el desarrollo es el siguiente:

$$\mathrm{SRTT}(K+1) = (0{,}2)\mathrm{RTT}(K+1) + (0{,}16)\mathrm{RTT}(K) + (0{,}218)\mathrm{RTT}(K-1) + \cdots$$

Cuanto más antigua es la observación, menos cuenta en el promedio.

Cuanto más pequeño es el valor de α, mayor es el peso dado a las observaciones más recientes. Para $\alpha = 0{,}5$, prácticamente todo el peso se le da a las cuatro o cinco observaciones más recientes, mientras que si $\alpha = 0{,}875$, el promediado se extiende alrededor de las diez observaciones más recientes. La ventaja de utilizar valores pequeños de α es que el promedio reflejará rápidamente un cambio rápido en las cantidades observadas. La desventaja radica en que, si se produce una subida breve en las cantidades observadas y después se vuelve a algún valor relativamente constante, el uso de valores pequeños de α producirá cambios fluctuantes en el promedio.

La Figura 20.11 compara el promediado simple con el promediado exponencial (para dos valores diferentes de α). En la parte (a) de la figura, el valor observado empieza con 1, crece gradualmente hasta el valor 10 y luego permanece ahí. En la parte (b) de la figura, el valor observado empieza en 20, decrece gradualmente hasta 10 y luego permanece ahí. Observe que el promediado exponencial sigue los cambios en el comportamiento del proceso más rápidamente que el promediado simple y que el valor más pequeño de α tiene como resultado reacciones más rápidas frente al cambio del valor observado.

La Ecuación (20.3) se utiliza en el RFC 793 para estimar el tiempo actual de ida y vuelta. Como se mencionó, el valor del temporizador debe establecerse a un valor algo mayor que el tiempo estimado de ida y vuelta. Una posibilidad consiste en utilizar un valor constante:

$$\text{RTO}(K + 1) = \text{SRTT}(K + 1) + \Delta$$

donde RTO es el temporizador de retransmisión (también conocido como el valor de expiración de retransmisión) y Δ es una constante. La desventaja de esto es que Δ no es proporcional a SRTT. Para valores altos de SRTT, Δ es relativamente pequeño y las fluctuaciones en el valor real de RTT producirán retransmisiones innecesarias. Para valores bajos de SRTT, Δ es relativamente grande y produce retardos innecesarios en la retransmisión de segmentos perdidos. De acuerdo a esto, el RFC 793 especifica la utilización de un temporizador cuyo valor es proporcional a SRTT, dentro de unos límites:

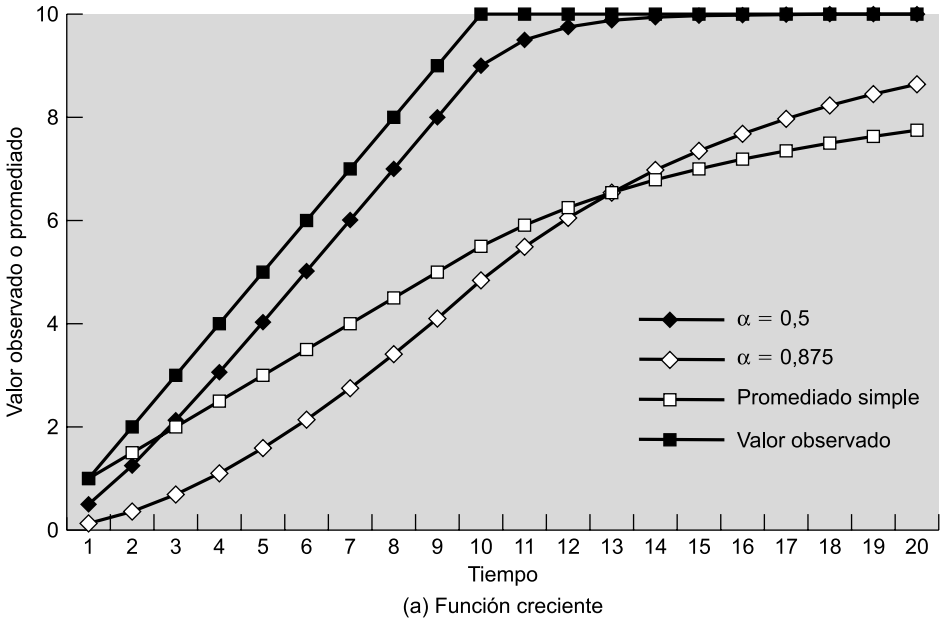
$$\text{RTO}(K + 1) = \text{MIN}(\text{UBOUND}, \text{MAX}(\text{LBOUND}, \beta \times \text{SRTT}(K + 1))) \qquad (20.4)$$

donde UBOUND y LBOUND son unos límites superior e inferior fijos preseleccionados para el valor del temporizador y β es una constante. El RFC 793 no recomienda valores específicos, pero da como valores de ejemplo los siguientes: α entre 0,8 y 0,9 y β entre 1,3 y 2,0.

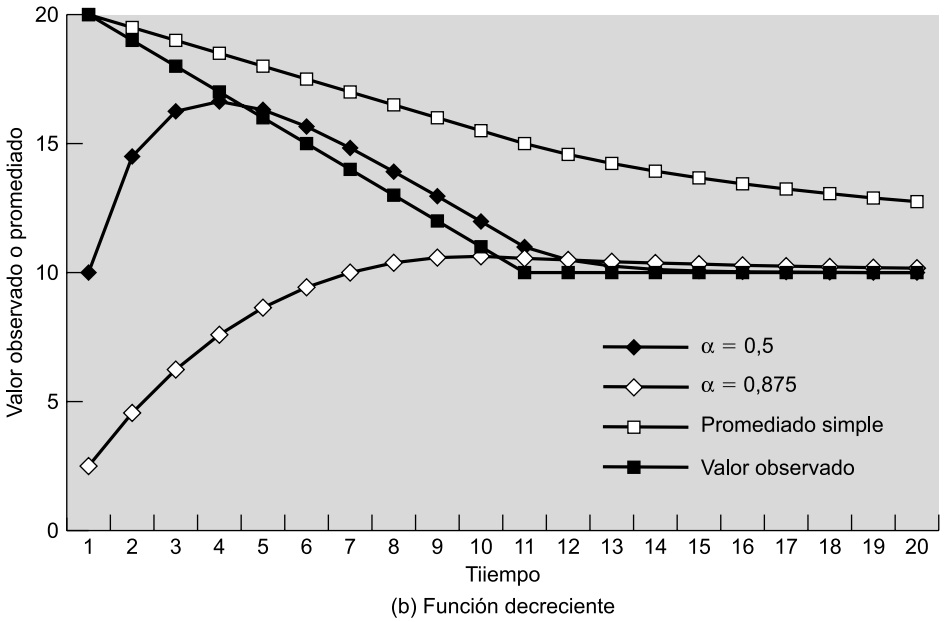
Estimación de la varianza del RTT (algoritmo de Jacobson)

La técnica especificada en el estándar TCP, y descrita en las Ecuaciones (20.3) y (20.4), habilita a una entidad TCP a adaptarse a los cambios del tiempo de ida y vuelta. Sin embargo, no trata bien una situación en la cual el tiempo de ida y vuelta exhiba una varianza relativamente elevada. [ZHAN86] señala tres fuentes de esta varianza:

1. Si la velocidad de transferencia de datos en una conexión TCP es relativamente baja, entonces el retardo de transmisión será relativamente alto comparado con el tiempo de propagación y la varianza en el RTT debida a la varianza en el tamaño de los datagramas IP será significativa. De esta forma, el estimador de SRTT está fuertemente influenciado por las características propias de los datos y no de la red.
2. La carga de tráfico y las condiciones en Internet pueden cambiar abruptamente debido al tráfico de otras fuentes, causando cambios bruscos en el RTT.



(a) Función creciente



(b) Función decreciente

Figura 20.11. Uso del promediado exponencial.

3. La entidad TCP par puede no confirmar cada segmento inmediatamente debido a su propio retardo de procesamiento o debido a que ejerce su privilegio de utilizar confirmaciones acumuladas.

La especificación original de TCP intenta considerar esta variabilidad multiplicando la estimación de RTT por un factor constante, como se muestra en la Ecuación (20.4). En un entorno estable, con una varianza baja de RTT, esta formulación tiene como resultado un valor innecesariamente alto

de RTO y en un entorno inestable un valor de $\beta = 2$ podría ser inadecuado para proteger contra retransmisiones innecesarias.

Una propuesta más efectiva consiste en estimar la variabilidad en los valores de RTT y utilizarla como entrada en el cálculo de una RTO. Una medida de variabilidad fácil de estimar es la desviación media, definida como

$$\text{MDEV}(X) = \text{E}[|X - \text{E}[X]|]$$

donde E[X] es el valor esperado de X.

Como se hizo con la estimación de RTT, se puede utilizar un promediado simple para estimar MDEV:

$$\begin{aligned}
\text{AERR}(K+1) &= \text{RTT}(K+1) - \text{ARTT}(K) \\
\text{ADEV}(K+1) &= \frac{1}{K+1} \sum_{i=1}^{K+1} |\text{AERR}(i)| \\
&= \frac{K}{K+1}\,\text{ADEV}(K) + \frac{1}{K+1}\,|\text{AERR}(K+1)|
\end{aligned}$$

donde ARTT(K) es la media simple definida en la Ecuación (20.1) y AERR(K) es la desviación media medida en el instante K.

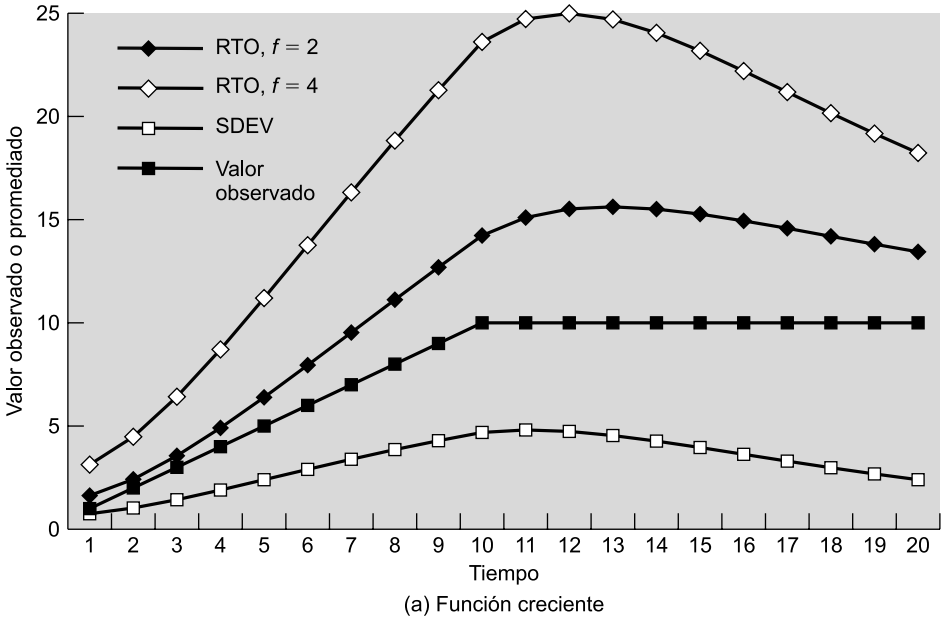
Como con la definición de ARRT, cada término de la sumatoria de ADEV tiene el mismo peso. Es decir, cada término se multiplica por la misma constante $1/(K + 1)$. De nuevo, querríamos dar un peso mayor a las medidas más recientes, ya que es más probable que reflejen el comportamiento futuro. Jacobson, que propuso la utilización de una estimación dinámica de la variabilidad en la estimación de RTT [JACO88], sugiere utilizar la misma técnica de suavizado exponencial que en el cálculo de SRTT. El algoritmo completo propuesto por Jacobson se puede expresar como sigue:

$$\begin{aligned}
\text{SRTT}(K+1) &= (1-g) \times \text{SRTT}(K) + g \times \text{RTT}(K+1) \\
\text{SERR}(K+1) &= \text{RTT}(K+1) - \text{SRTT}(K) \\
\text{SEV}(K+1) &= (1-h) \times \text{SDEV}(K) + h \times |\text{SERR}(K+1)| \\
\text{RTO}(K+1) &= \text{SRTT}(K+1) + f \times \text{SDEV}(K+1)
\end{aligned} \tag{20.5}$$

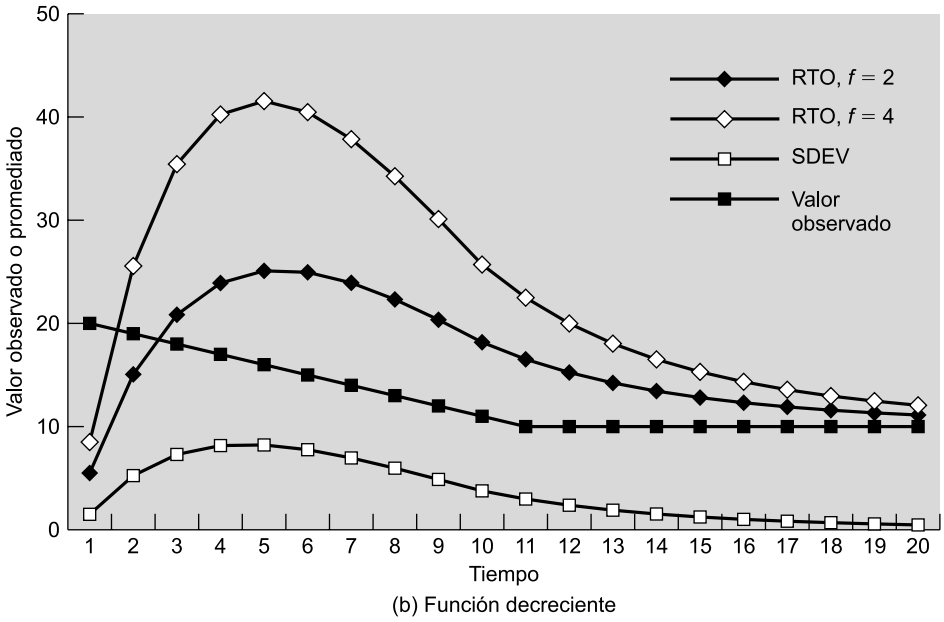
Como en la definición del RFC 793 (Ecuación (20.3)), SRTT es una estimación exponencial suavizada de RTT, con $(1 - g)$ equivalente a α. Ahora, sin embargo, en lugar de multiplicar la estimación SRTT por una constante (Ecuación (20.4)), se suma a SRTT un múltiplo de la desviación media estimada para formar el temporizador de retransmisión. Basándose en sus experimentos de temporización, Jacobson propuso en su artículo original [JACO88] los siguientes valores para las constantes:

$$\begin{aligned}
g &= 1/8 = 0{,}125 \\
h &= 1/4 = 0{,}25 \\
f &= 2
\end{aligned}$$

Después de investigaciones posteriores [JACO90], recomendó cambiar el valor de f a 4, siendo éste el valor estándar utilizado en las implementaciones actuales.



(a) Función creciente



(b) Función decreciente

Figura 20.12. Cálculo del RTO de Jacobson.

La Figura 20.12 muestra el uso de la Ecuación (20.5) sobre el mismo conjunto de datos que se utilizó en la Figura 20.11. Una vez que el tiempo de llegada se estabiliza, la estimación de la variación SDEV decae. Los valores de RTO para ambos casos ($f = 2$ y $f = 4$) son bastante conservadores mientras que RTT esté cambiando, pero comienzan a converger a RTT cuando se estabiliza.

La experiencia ha demostrado que el algoritmo de Jacobson puede mejorar significativamente el rendimiento de TCP. Sin embargo, no basta por sí solo. Se deben considerar otros dos factores:

1. ¿Qué valor de RTO se debe utilizar para un segmento retransmitido? Para este caso se utiliza el algoritmo de decaimiento exponencial de RTO.
2. ¿Qué muestras se deben utilizar como entrada al algoritmo de Jacobson? El algoritmo de Karn determina qué muestras se han de utilizar.

Decaimiento exponencial de RTO

Cuando expira un temporizador en el emisor TCP, éste debe retransmitir el segmento correspondiente. El RFC 793 supone que se va a utilizar el mismo RTO para este segmento retransmitido. Sin embargo, ya que el que expire el temporizador se debe probablemente a la congestión de la red, manifestada como el descarte de un paquete o un largo retardo en el tiempo de ida y vuelta, mantener el mismo valor de RTO no es aconsejable.

Considere el siguiente escenario. Existen varias conexiones TCP activas de varias fuentes enviando tráfico a una interconexión de redes. Aparece la congestión en una región, de forma que los segmentos en muchas de esas conexiones se pierden o retrasan por encima del tiempo RTO de las conexiones. Por tanto, casi al mismo tiempo, muchos segmentos serán retransmitidos por la interconexión de redes, manteniendo o incluso incrementando la congestión. Todas las fuentes esperan un tiempo RTO (local a cada conexión) y retransmiten de nuevo. Este patrón de comportamiento podría causar una condición de congestión continua.

Una política más sensible dicta que una fuente TCP incremente su RTO cada vez que se retransmita el mismo segmento. Esto se conoce como proceso de *decaimiento*. En el escenario del párrafo anterior, después de la primera retransmisión de un segmento de cada conexión afectada, todas las fuentes TCP esperarán un tiempo mayor antes de intentar la segunda retransmisión. Esto puede darle tiempo a la interconexión de redes para despejar la congestión actual. Si se necesita una segunda retransmisión, cada fuente TCP esperará un tiempo todavía mayor antes de que expire el temporizador correspondiente para una tercera retransmisión, dando a la interconexión un periodo aún mayor para recuperarse.

Una técnica simple para implementar el decaimiento de RTO consiste en multiplicar el RTO de un segmento por un valor constante para cada retransmisión:

$$\text{RTO} = q \times \text{RTO} \tag{20.6}$$

La Ecuación (20.6) hace que el RTO crezca exponencialmente con cada retransmisión. El valor de q más comúnmente utilizado es 2. Con este valor, la técnica se conoce como *decaimiento exponencial binario*. Ésta es la misma técnica que se utiliza en el protocolo CSMA/CD de Ethernet (*véase* Capítulo 16).

Algoritmo de Karn

Si no se retransmite ningún segmento, el proceso de muestreo para el algoritmo de Jacobson es directo. El RTT de cada segmento se puede incluir en los cálculos. Sin embargo, suponga que expira el temporizador de un segmento, por lo que debe retransmitirse. Si se recibe una confirmación posterior, existen dos posibilidades:

1. Se trata del ACK de la primera transmisión del segmento. En este caso, el RTT es simplemente mayor que el esperado, pero es un reflejo preciso de las condiciones de la red.
2. Se trata del ACK de la segunda transmisión.

La entidad emisora TCP no puede distinguir entre estos dos casos. Si se trata del segundo caso y la entidad TCP mide simplemente el RTT desde la primera transmisión hasta la recepción del ACK, el tiempo medido será demasiado alto. El RTT medido será del orden del RTT actual más el RTO. Utilizar este falso RTT con el algoritmo de Jacobson producirá un valor alto innecesario de SRTT y, por tanto, de RTO. Es más, este efecto se propaga varias iteraciones, ya que el valor de SRTT de una iteración es un valor de entrada en la siguiente iteración.

Un enfoque incluso peor consistiría en medir el RTT de la segunda transmisión hasta la recepción del ACK. Si éste es en efecto el ACK de la primera transmisión, entonces el RTT medido sería demasiado pequeño, produciendo un valor demasiado bajo de SRTT y de RTO. Esto es probable que tenga un efecto de realimentación positiva, causando retransmisiones adicionales y medidas falsas.

El algoritmo de Karn [KARN91] resuelve este problema mediante las siguientes reglas:

1. No utilizar el RTT medido para un segmento retransmitido para actualizar SRTT y SDEV [Ecuación (20.5)].
2. Calcular el RTO de decaimiento utilizando la Ecuación (20.6) cuando se produzca una retransmisión.
3. Utilizar el valor del RTO de decaimiento para segmentos sucesivos hasta que llegue una confirmación para un segmento que no se haya retransmitido.

Cuando se recibe una confirmación para un segmento que no se ha retransmitido, se activa de nuevo el algoritmo de Jacobson para calcular valores futuros de RTO.

GESTIÓN DE VENTANA

Además de las técnicas para mejorar la efectividad del temporizador de retransmisión, se han examinado varias aproximaciones para gestionar la ventana de emisión. El tamaño de la ventana de emisión de TCP puede tener un efecto decisivo para que TCP pueda ser utilizado eficientemente sin causar congestión. Discutiremos dos técnicas que se encuentran virtualmente en todas las implementaciones recientes de TCP: el arranque lento y el ajuste dinámico de la ventana en caso de congestión[3].

Arranque lento

Cuanto mayor es la ventana de emisión de TCP, más segmentos puede enviar la fuente TCP antes de que deba esperar una confirmación. Esto puede crear un problema cuando se establece por primera vez una conexión TCP, ya que la entidad TCP es libre de vaciar la ventana de datos completa en la red.

Una estrategia que se podría seguir consiste en que el emisor TCP empezara a enviar con una ventana relativamente grande pero no con su máximo tamaño, esperando aproximarse al tamaño máximo que sería proporcionado por la conexión finalmente. Este esquema es arriesgado, ya que el emisor podría inundar la interconexión de redes con muchos segmentos antes de darse cuenta por los temporizadores de que el flujo era excesivo. En lugar de eso, se necesita algún medio para

[3] Estos algoritmos fueron desarrollados por Van Jacobson [JACO88] y son descritos además en el RFC 2581. Van Jacobson utiliza unidades de segmentos TCP, mientras que en el RFC 2581 se trabaja principalmente en unidades de octetos de datos TCP, con alguna referencia a cálculos en unidades de segmentos. Nosotros seguimos el desarrollo de [JACO88].

expandir gradualmente la ventana hasta que se reciban las confirmaciones. Éste es el propósito del mecanismo de arranque lento.

En el arranque lento, la transmisión TCP está restringida por la siguiente relación:

$$awnd = \text{MIN}[crédito, cwnd] \tag{20.7}$$

donde

awnd = ventana permitida, en segmentos. Éste es el número de segmentos que TCP tiene actualmente permitido enviar sin recibir confirmaciones adicionales.

cwnd = ventana de congestión, en segmentos. Ventana utilizada por TCP durante el inicio y para reducir el flujo durante los periodos de congestión.

crédito = la cantidad de créditos concedidos y no utilizados en la confirmación más reciente, en segmentos. Cuando se recibe una confirmación, este valor se calcula como *ventana*/*tamaño_de_segmento*, donde *ventana* es un campo del segmento TCP recibido (la cantidad de datos que está dispuesta a aceptar la entidad TCP par).

La entidad TCP inicializa *cwnd* = 1 cuando se abre una conexión. Es decir, a TCP sólo se le permite enviar un segmento y después debe esperar una confirmación antes de enviar un segundo segmento. Cada vez que reciba una confirmación para datos nuevos, se incrementa el valor de *cwnd* en una unidad, hasta algún valor máximo.

En efecto, el mecanismo de arranque lento sondea la interconexión de redes para asegurarse de que la entidad TCP no esté enviando demasiados segmentos en un entorno ya congestionado. Conforme van llegando las confirmaciones, a TCP se le permite abrir su ventana hasta que el flujo se controle mediante las confirmaciones que se reciben, en lugar de mediante *cwnd*.

El término arranque lento es un nombre poco apropiado, ya que *cwnd* crece en realidad exponencialmente. Cuando llega el primer ACK, TCP abre *cwnd* hasta 2 y puede enviar dos segmentos. Cuando estos dos segmentos se confirman, TCP puede desplazar la ventana 1 segmento e incrementar *cwnd* en uno por cada ACK que llega. Por tanto, en este punto TCP puede enviar cuatro segmentos. Cuando se confirmen estos cuatro segmentos, TCP podrá enviar ocho segmentos.

Ajuste dinámico de la ventana en caso de congestión

Se ha comprobado que el algoritmo de arranque lento funciona de forma efectiva para inicializar una conexión. Permite a TCP determinar rápidamente un tamaño de ventana razonable para la conexión. ¿No sería útil la misma técnica cuando haya un incremento de la congestión? En particular, suponga que una entidad TCP inicia una conexión y ejecuta el procedimiento de arranque lento. En algún punto, antes o después de que *cwnd* alcance el tamaño de créditos asignados por el otro extremo, se pierde un segmento (expira un temporizador). Esto es una señal de que se está produciendo congestión. Pero no está claro cómo de severa es la congestión. Por tanto, un procedimiento prudente sería inicializar *cwnd* a 1 y comenzar el procedimiento de arranque lento de nuevo.

Éste parece un procedimiento conservador razonable, pero en realidad no es lo bastante conservador. Jacobson [JACO88] señala que «es fácil llevar una red a la saturación, pero es difícil para la red recuperarse». En otras palabras, una vez que la congestión se produce, puede transcurrir un largo intervalo de tiempo hasta que ésta desaparezca[4]. De esta forma, el crecimiento exponencial

[4] Kleinrock se refiere a este fenómeno como el efecto de larga cola en periodos punta. *Véanse* las Secciones 2.7 y 2.10 de [KLEI76] para un estudio detallado.

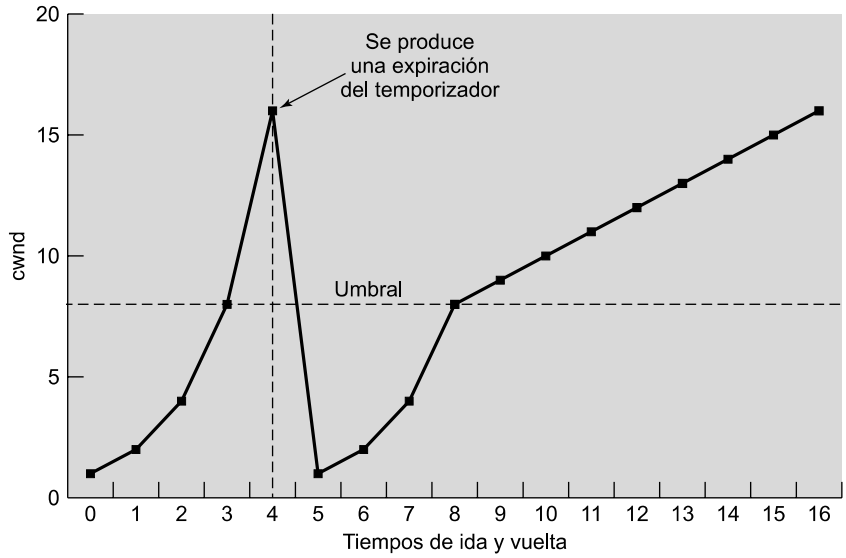


Figura 20.13. Ilustración del arranque lento y la supresión de congestión.

de *cwnd* bajo el arranque lento puede ser demasiado agresivo y empeorar la congestión. En lugar de esto, Jacobson propuso el uso del arranque lento para comenzar, seguido de un crecimiento lineal de *cwnd*. Cuando expira un temporizador las reglas son las siguientes:

1. Establecer un umbral de arranque lento igual a la mitad de la ventana de congestión actual. Es decir, hacer *ssthresh* = *cwnd*/2.
2. Establecer *cwnd* = 1 y ejecutar el procedimiento de arranque lento hasta que *cwnd* = *ssthresh*. En esta fase, *cwnd* se incrementa en 1 por cada ACK recibido.
3. Para *cwnd* $\geqslant$ *ssthresh*, incrementar *cwnd* en uno por cada tiempo de ida y vuelta.

La Figura 20.13 muestra este comportamiento. Observe que le lleva 11 veces el tiempo de ida y vuelta recuperar el nivel *cwnd* que inicialmente se consiguió con 4 veces el tiempo de ida y vuelta.

20.4. UDP

Además de TCP, existe otro protocolo en la capa de transporte que se usa comúnmente como parte del conjunto de protocolos TCP/IP: el protocolo de datagrama de usuario (UDP, *User Datagram Protocol*), especificado en el RFC 768. UDP proporciona un servicio no orientado a conexión para los procedimientos de la capa de aplicación. Así, UDP es básicamente un servicio no fiable: no se garantizan la entrega y la protección contra duplicados. En contrapartida, se reduce la sobrecarga del protocolo, lo que puede ser adecuado en muchos casos. Un ejemplo de uso de UDP se tiene en el contexto de la gestión de red, como se describe en el Capítulo 22.

La fortaleza del enfoque orientado a conexión es clara. Permite características relacionadas con la conexión, como son el control de flujo, el control de errores y la entrega ordenada. Sin embargo, un servicio no orientado a conexión es más apropiado para algunos contextos. En capas inferiores (interconexión y red) es más robusto (por ejemplo, *véase* la discusión de la Sección 10.6). Además,

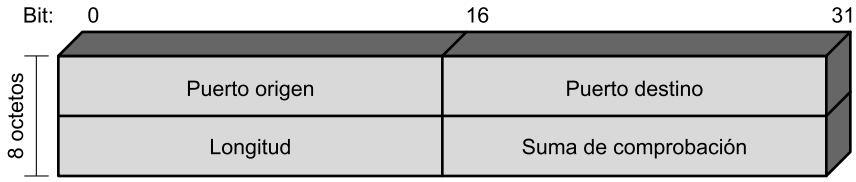


Figura 20.14. Cabecera UDP.

representa un «menor común denominador» del servicio que esperan las capas superiores. Pero, incluso a nivel de transporte y superiores, existe una justificación para un servicio no orientado a conexión. Existen casos en los que la sobrecarga del establecimiento y cierre de la conexión no están justificados o son incluso contraproducentes. Algunos ejemplos son:

- **Recolección de datos internos:** implica un muestreo activo o pasivo de fuentes de datos, como los procedentes de sensores e informes automáticos de autocomprobación de seguridad de equipos o componentes de red. En una situación de monitorización en tiempo real, la pérdida ocasional de una unidad de datos no causaría ningún desastre, ya que el siguiente informe debe llegar en breve.
- **Diseminación de datos externos:** incluye la difusión de mensajes a los usuarios de la red, el anuncio de un nuevo nodo o el cambio de la dirección de un servicio y la distribución de los valores de reloj de tiempo real.
- **Petición/respuesta:** aplicaciones en las cuales un servidor común proporciona un servicio de transacción a varios usuarios TS distribuidos y para el cual usar una secuencia del tipo petición/respuesta es usual. El uso del servicio se regula en la capa de aplicación y las conexiones de capas inferiores son frecuentemente innecesarias y molestas.
- **Aplicaciones en tiempo real:** como aplicaciones de voz y de telemedida, que llevan consigo el requisito de utilizar cierto grado de redundancia y/o transmisión en tiempo real. Estos requisitos no pueden tener funciones orientadas a conexión como la retransmisión.

Así, tienen cabida en la capa de transporte tanto servicios orientados a conexión como servicios no orientados a conexión.

UDP se sitúa encima de IP. Ya que es no orientado a conexión, UDP tiene muy pocas tareas que llevar a cabo. Esencialmente, incorpora a IP la capacidad de un direccionamiento de puerto. Esto se ve mejor examinando la cabecera UDP mostrada en la Figura 20.14. La cabecera incluye un puerto origen y un puerto destino. El campo de longitud contiene la longitud de todo el segmento UDP, incluyendo la cabecera y los datos. La suma de comprobación es el mismo algoritmo usado en TCP e IP. Para UDP, la suma de comprobación se aplica al segmento UDP entero más una pseudocabecera incorporada a la cabecera UDP en el momento del cálculo, que es la misma que la utilizada en TCP. Si se detecta un error, el segmento se descarta sin tomar ninguna medida adicional.

El campo de suma de comprobación en UDP es opcional. Si no se utiliza, se le asigna el valor cero. Sin embargo, hay que indicar que la suma de comprobación de IP se aplica sólo a la cabecera IP y no al campo de datos, que en este caso está compuesto por la cabecera UDP y los datos de usuario. Así, si UDP no efectúa ningún cálculo de suma de comprobación, los datos de usuario no se verifican.

20.5. LECTURAS RECOMENDADAS

Quizá el mejor estudio de las distintas estrategias de TCP para el control de flujo y de la congestión se encuentre en [STEV94]. Un artículo fundamental para comprender las cuestiones implicadas es el clásico [JACO88].

JACO88 Jacobson, V. «Congestion Avoidance and Control». *Proceedings, SIGCOMM'88, Computer Communication Review,* agosto de 1988; reimpreso en *Computer Communication Review*, enero de 1995; una versión revisada puede encontrarse en ftp.ee.lbl.gov/papers/congavoid.ps.Z.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols.* Reading, MA: Addison-Wesley, 1994.

20.6. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

algoritmo de Karn
arranque lento
control de congestión TCP
control de flujo
crédito
detección de duplicados
estrategia de retransmisión
flujo de datos forzado
multiplexación
número de secuencia
opciones en los criterios de implementación TCP
promediado exponencial
protocolo de control de transmisión (TCP)
protocolo de datagrama de usuario (UDP)
protocolo de transporte
puerto
señalización de datos urgentes
socket
suma de comprobación

CUESTIONES DE REPASO

20.1. ¿Qué elementos de direccionamiento son necesarios para especificar un usuario de servicio de transporte (TS) destino?

20.2. Describa cuatro estrategias por las que un usuario TS emisor pueda averiguar la dirección de un usuario TS receptor.

20.3. Explique el uso de la multiplexación en el contexto de un protocolo de transporte.

20.4. Describa brevemente el esquema de créditos utilizado por TCP para el control de flujo.

20.5. ¿Cuál es la diferencia principal entre el esquema de créditos de TCP y el esquema de control de flujo de ventana deslizante utilizada por muchos otros protocolos, como por ejemplo HDLC?

20.6. Explique los mecanismos de diálogo en dos y tres pasos.

20.7. ¿Cuál es el beneficio del mecanismo de diálogo en tres pasos?

20.8. Defina las características de urgencia y forzado de TCP.

20.9. ¿Qué es una opción en los criterios de implementación de TCP?

20.10. ¿Cómo puede utilizarse TCP para tratar la congestión de red o de interconexión de red?

20.11. ¿Qué proporciona UDP que no ofrezca IP?

EJERCICIOS

20.1. Es una práctica común en la mayoría de los protocolos de transporte (en realidad, en la mayoría de los protocolos de todas las capas) que los datos y la señalización de control se multiplexen sobre el mismo canal lógico en cada conexión por usuario. Una alternativa consiste en establecer una única conexión de control de transporte entre cada par de entidades de transporte que se comuniquen. Esta conexión se usaría para transmitir las señales de control de todas las conexiones de los usuarios de transporte entre las dos entidades. Discuta las implicaciones de esta estrategia.

20.2. La discusión sobre control de flujo con un servicio de red fiable, referido como mecanismo de contrapresión, utiliza un protocolo de control de flujo de una capa inferior. Discuta las desventajas de esta estrategia.

20.3. Dos entidades de transporte de comunican a través de una red fiable. Supongamos que el tiempo normalizado para transmitir un segmento es igual a 1. Supongamos que el retardo de propagación extremo a extremo vale 3 y que la entrega de un segmento recibido al usuario de transporte requiere un tiempo de 2. El emisor tiene inicialmente concedido un crédito de siete segmentos. El receptor utiliza un criterio de control de flujo conservador y actualiza su asignación de créditos en cuanto puede. ¿Cuál es el máximo rendimiento alcanzable?

20.4. Dibuje un diagrama similar al de la Figura 20.4 para los siguientes casos (suponga un servicio de red fiable ordenado):

a) Cierre de la conexión: activo/pasivo.

b) Cierre de la conexión: activo/activo.

c) Rechazo de la conexión.

d) Cancelación de la conexión: un usuario emite un *Open* a un usuario que está preparado y entonces emite un *Close* antes de que se intercambie ningún dato.

20.5. Con un servicio de red fiable y ordenado, ¿son estrictamente necesarios los números de secuencia de los segmentos? ¿Qué capacidad se pierde sin ellos?

20.6. Considere un servicio de red orientado a conexión que sufre un reinicio. ¿Cómo podría ser tratado por un protocolo de transporte que suponga que el servicio de red es fiable excepto en el caso de un reinicio?

20.7. La discusión de la política de retransmisión hizo referencia a tres problemas asociados con el cálculo dinámico del valor del temporizador. ¿Qué modificaciones sobre la política ayudarían a aliviar estos problemas?

20.8. Considere un protocolo de transporte que usa un servicio de red orientado a conexión. Suponga que ese protocolo de transporte utiliza un esquema de asignación de créditos para el control de flujo y que el protocolo de red usa un esquema de ventana deslizante. ¿Qué relación, si existe, debería haber entre la ventana dinámica del protocolo de transporte y la ventana fija del protocolo de red?

20.9. En una red que tiene un tamaño máximo de paquete de 128 bytes, un tiempo de vida máximo de 30 s y un número de secuencia de paquetes de 8 bits, ¿cuál es la máxima tasa de transmisión de datos por conexión?

20.10. ¿Es posible que se produzca un bloqueo mutuo utilizando un diálogo en dos pasos en lugar de un diálogo en tres pasos? Dé un ejemplo o demuéstrelo en caso contrario.

20.11. A continuación, se enumeran cuatro estrategias que se pueden utilizar para proporcionar a un usuario de transporte las direcciones de un usuario de transporte destino. Para cada una, describa una analogía con el usuario del servicio de correo postal.

a) Conocer la dirección de antemano.

b) Hacer uso de una dirección «bien conocida».

c) Utilizar un servidor de nombres.

d) El destinatario se genera al realizar la solicitud.

20.12. En un esquema de créditos para control de flujo como el de TCP, ¿qué provisión de créditos se podría hacer para la asignación de créditos que se pierdan o se desordenen durante la transmisión?

20.13. ¿Qué ocurre en la Figura 20.3 si llega un SYN mientras el usuario solicitado está en el estado *CLOSED*? ¿Hay alguna forma de llamar la atención del usuario cuando no esté preparado?

20.14. En la discusión sobre el cierre de la conexión con referencia a la Figura 20.8, se estableció que además de recibir una confirmación de su segmento FIN y enviar una confirmación del segmento FIN recibido, una entidad TCP debe esperar un intervalo de tiempo igual al doble del máximo tiempo de vida esperado de un segmento (el estado *TIME WAIT*). La recepción de un ACK de su segmento FIN le asegura que todos los segmentos que ha enviado han sido recibidos por el otro extremo. El envío de un ACK del segmento FIN del otro extremo asegura a la otra entidad que todos sus segmentos han sido recibidos. Dé una razón por la que se necesite aún esperar antes de cerrar la conexión.

20.15. Normalmente, el campo «ventana» de la cabecera TCP da una asignación de créditos en octetos. Cuando se utiliza la opción de «escalado de ventana», el valor del campo «ventana» se multiplica por 2^F, donde F es el valor de la opción de escalado de ventana. El valor máximo de F que acepta TCP es 14. ¿Por qué se limita esta opción a 14?

20.16. La elección de un valor inicial del estimador original de SRTT de TCP constituye un problema. En ausencia de alguna información especial sobre las condiciones de la red, la opción habitual es la de elegir un valor arbitrario, como 3 segundos, y esperar que converja rápidamente a un valor preciso. Si la estimación es demasiado baja, TCP llevará a cabo retransmisiones innecesarias. Si es demasiado alta, TCP esperará demasiado tiempo antes de retransmitir en caso de que el primer segmento se pierda. Es más, la convergencia puede ser lenta, como indica este problema.

a) Elija $\alpha = 0{,}85$ y SRTT(0) = 3 segundos, suponga que todos lo valores de RTT medidos son iguales a 1 segundo y que no se producen pérdidas de paquetes. ¿Cuál es el valor de SRTT(19)? *Sugerencia:* la Ecuación (20.3) se puede reescribir para simplificar los cálculos, utilizando la expresión $(1 - \alpha^n)/(1 - \alpha)$.

b) Sea ahora SRTT(0) = 1 segundo y suponga que los valores medidos de RTT son 3 segundos y que no se produce pérdida de paquetes. ¿Cuál es el valor de SRTT(19)?

20.17. Una mala implementación del esquema de ventana deslizante de TCP puede llevar a un rendimiento extremadamente malo. Existe un fenómeno conocido como el «síndrome de la ventana absurda» (SWS, *Silly Window Sindrome*), que puede fácilmente causar una degradación del rendimiento en varios factores de 10. Como ejemplo de SWS, considere una aplicación que está ocupada en la transferencia de un fichero largo y que TCP está transfiriendo el fichero en segmentos de 200 octetos. El receptor inicialmente asigna un crédito

de 1.000. El emisor agota esta ventana con 5 segmentos de 200 octetos. Ahora suponga que el receptor devuelve una confirmación por cada segmento y proporciona un crédito adicional de 200 octetos por cada segmento recibido. Desde el punto de vista del receptor, esto abre la ventana de nuevo a 1.000 octetos. Sin embargo, desde el punto de vista del emisor, si la primera confirmación llega tras haber enviado cinco segmentos, se dispone de una ventana de sólo 200 octetos. Suponga que en algún momento el receptor calcula una ventana de 200 octetos pero tiene sólo 50 octetos para enviar hasta llegar a un punto de forzado. Por tanto, envía 50 octetos en un segmento, seguido de 150 octetos en el siguiente segmento, y reanuda la transmisión de segmentos de 200 octetos. ¿Qué podría ahora ocurrir para dar lugar a un problema de rendimiento? Plantee el SWS en términos más generales.

20.18. TCP impone que tanto el receptor como el emisor incorporen mecanismos para hacer frente al SWS.

a) Sugiera una estrategia para el receptor. *Sugerencia:* permita al receptor «mentir» sobre la capacidad de memoria temporal de que dispone bajo ciertas circunstancias. Plantee una regla razonable experimental para esto.

b) Sugiera una estrategia para el emisor. *Sugerencia:* considere la relación entre la ventana máxima posible de envío y lo que hay disponible para enviar.

20.19. En la Ecuación (20.5), reescriba la definición de SRTT($K+1$) en función de SERR($K+1$). Interprete el resultado.

20.20. Una entidad TCP abre una conexión y utiliza el arranque lento. Aproximadamente, ¿cuántos tiempos de ida y vuelta se necesitan antes de que TCP pueda enviar N segmentos?

20.21. Aunque el arranque lento con supresión de congestión es una técnica efectiva para hacer frente a la congestión, puede traducirse en largos tiempos de recuperación en redes de alta velocidad, como demuestra este problema:

a) Suponga un retardo de ida y vuelta de 60 ms (lo que podría ocurrir a través de un continente), un enlace con un ancho de banda disponible de 1 Gbps y un tamaño de segmento de 576 octetos. Determine el tamaño de ventana necesario para mantener lleno el cauce y el tiempo que tardaría en alcanzar el tamaño de ventana después de la expiración del temporizador utilizando el criterio de Jacobson.

b) Repita (a) para un tamaño de ventana de 16 kbytes.

CAPÍTULO 21

Seguridad en redes

21.1. Requisitos de seguridad y ataques
Ataques pasivos
Ataques activos

21.2. Privacidad con cifrado simétrico
Cifrado simétrico
Algoritmos de cifrado
Localización de los dispositivos de cifrado
Distribución de claves
Relleno de tráfico

21.3. Autenticación de mensajes y funciones de dispersión (*hash*)
Alternativas para la autenticación de mensajes
Funciones de dispersión seguras
La función de dispersión segura SHA-1

21.4. Cifrado de clave pública y firmas digitales
Cifrado de clave pública
Firma digital
El algoritmo de cifrado de clave pública RSA
Gestión de claves

21.5. Capa de *sockets* segura (SSL) y capa de transporte segura (TLS)
Arquitectura SSL
Protocolo de registro de SSL
Protocolo de cambio de especificación de cifrado
Protocolo de alerta
Protocolo de negociación bilateral

21.6. Seguridad en IPv4 e IPv6
Aplicaciones de IPSec
Ámbito de IPSec
Asociaciones de seguridad
Cabecera de autenticación
Encapsulado de la carga útil de seguridad

21.7. Lecturas y sitios web recomendados

21.8. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- Las amenazas a la seguridad de la red se dividen en dos categorías: las **amenazas pasivas**, llamadas a veces escuchas, que suponen el intento de un atacante de obtener información relativa a una comunicación, y las **amenazas activas, que** suponen alguna modificación de los datos transmitidos o la creación de transmisiones falsas.
- Hasta ahora, la herramienta automática más importante para la seguridad en red y de las comunicaciones es el **cifrado**. En el **cifrado simétrico**, dos entidades comparten una sola clave de cifrado/descifrado. El principal reto del cifrado simétrico consiste en la distribución y protección de las claves. Un esquema de **cifrado de clave pública** supone el uso de dos claves, una para el cifrado y la otra para el descifrado. La parte que generó el par de claves mantiene privada una de ellas y difunde la otra.
- El cifrado simétrico y el cifrado de clave pública se suelen combinar en aplicaciones de red seguras. El cifrado simétrico se utiliza para cifrar los datos transmitidos, utilizando una clave de un solo uso o clave temporal de sesión. La clave de sesión la puede distribuir un centro de distribución de claves de confianza o puede ser transmitida protegida mediante un cifrado de clave pública. El cifrado de clave pública también se utiliza para crear firmas digitales, que pueden autenticar la fuente de los mensajes transmitidos.
- La capa de *sockets* segura (SSL), y el estándar de Internet posterior, conocido como capa de transporte segura (TLS), proporcionan servicios de seguridad para transacciones web.
- Una mejora en la seguridad empleada con IPv4 e IPv6, llamada IPSec, proporciona mecanismos de privacidad y autenticación.

Los requisitos de la **seguridad de la información** dentro de una organización han sufrido dos cambios principales en las últimas décadas. Antes de que se extendiera la utilización de los equipos de procesamiento de datos, la seguridad de la información valiosa para la organización se proporcionaba fundamentalmente por medios físicos y administrativos. Como ejemplo del primer tipo de medios sirva el empleo de robustos archivadores con cerrojo de combinación para almacenar los documentos importantes. Un ejemplo del segundo es el uso de procedimientos de investigación del personal durante el proceso de contratación.

Con la introducción de los computadores, se hizo evidente la necesidad de herramientas automáticas para proteger ficheros y otra información almacenada en el computador. Éste es especialmente el caso de los sistemas compartidos, como los sistemas multiusuario. Esta necesidad se acentúa en los sistemas a los que se pueda acceder desde redes de datos o redes de telefonía públicas. El término genérico del conjunto de herramientas diseñadas para proteger los datos y frustrar las actividades de los piratas de la computación es **seguridad en computadores**. Aunque constituye un tema muy importante, se encuentra fuera del alcance de este libro.

El segundo cambio relevante que ha afectado a la seguridad es la introducción de sistemas distribuidos y la utilización de redes y servicios de comunicación para transportar datos entre terminales de usuario y computadores y de computador a computador. Las medidas de **seguridad en red** son necesarias para proteger los datos durante su transmisión y garantizar que los datos transmitidos sean auténticos.

La tecnología esencial subyacente, virtualmente, en todas las aplicaciones de seguridad en redes y computadores es el cifrado. Se utilizan dos técnicas fundamentales: cifrado simétrico y

cifrado de clave pública, también conocido como cifrado asimétrico. Conforme examinemos las diversas técnicas de seguridad en red, iremos explorando los dos tipos de cifrado.

Este capítulo comienza con una visión global de los requisitos de seguridad en red. A continuación, se examinará el cifrado simétrico y su utilización para proporcionar privacidad. A esto le sigue una discusión sobre la autenticación de mensajes. Se examinará el uso del cifrado de clave pública y las firmas digitales. El capítulo termina con un estudio de las características de seguridad de SSL e IPSec.

21.1. REQUISITOS DE SEGURIDAD Y ATAQUES

Para entender los tipos de amenazas a la seguridad que existen, necesitamos partir de una definición de requisitos en seguridad. La seguridad en computadores y en redes implica cuatro requisitos:

- **Privacidad:** se requiere que sólo entidades autorizadas puedan tener un acceso a la información. Este tipo de acceso incluye la impresión, la visualización y otras formas de revelado, incluyendo el simple hecho de dar a conocer la existencia de un objeto.
- **Integridad:** se requiere que los datos sean modificados solamente por partes autorizadas. La modificación incluye la escritura, la modificación, la modificación del estado, la supresión y la creación.
- **Disponibilidad:** se requiere que los datos estén disponibles para las partes autorizadas.
- **Autenticidad:** se requiere que un computador o servicio sea capaz de verificar la identidad de un usuario.

Una forma útil de clasificar los ataques a la seguridad (RFC 2828) es en términos de *ataques pasivos* y *ataques activos*. Un ataque pasivo intenta averiguar o hacer uso de información del sistema, pero sin afectar a los recursos del mismo. Un ataque activo intenta alterar los recursos del sistema o influir en su funcionamiento.

ATAQUES PASIVOS

Los ataques pasivos consisten en escuchas o monitorizaciones de las transmisiones. La meta del oponente es la de obtener la información que está siendo transmitida. La divulgación del contenido de un mensaje y el análisis de tráfico constituyen dos tipos de ataques pasivos.

La **divulgación del contenido de un mensaje** se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico o un fichero transferido pueden contener información sensible o confidencial. Por ello, desearíamos impedir que un oponente averigüe el contenido de estas transmisiones.

Un segundo tipo de ataque pasivo, el **análisis de tráfico**, es más sutil. Suponga que disponemos de un medio para enmascarar el contenido de los mensajes u otro tipo de tráfico de información, de forma que aunque los oponentes capturasen el mensaje, no podrían extraer la información del mismo. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección por cifrado, el oponente podría todavía observar el patrón de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información podría serle útil para averiguar la naturaleza de la comunicación que se está realizando.

Los ataques pasivos son muy difíciles de detectar, ya que no suponen la alteración de los datos. Normalmente, el tráfico de mensajes es enviado y recibido de forma aparentemente normal y ni el emisor ni el receptor son conscientes de que un tercero haya leído los mensajes u observado el patrón de tráfico. Sin embargo, es factible impedir el éxito de estos ataques, usualmente mediante cifrado. De esta manera, el énfasis en la defensa contra estos ataques se centra en la prevención en lugar de en la detección.

ATAQUES ACTIVOS

Los ataques activos suponen alguna modificación del flujo de datos o la creación de flujos falsos. Los podemos clasificar en 4 categorías: enmascaramiento, retransmisión, modificación de mensajes y denegación de servicio.

Un **enmascaramiento** tiene lugar cuando una entidad pretende ser otra entidad diferente. Un ataque por enmascaramiento normalmente incluye una de las otras formas de ataques activos. Por ejemplo, se pueden capturar secuencias de autenticación y retransmitirlas después de que tenga lugar una secuencia válida, permitiendo así obtener privilegios adicionales a otra entidad autorizada con escasos privilegios mediante la suplantación de la entidad que los posee.

La **retransmisión** supone la captura pasiva de unidades de datos y su retransmisión posterior para producir un efecto no autorizado.

La **modificación de mensajes** significa sencillamente que algún fragmento de un mensaje legítimo se modifica o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo, un mensaje con un significado «Permitir a Juan García leer el fichero confidencial de cuentas» se modifica para tener el significado «Permitir a Alfredo Castaño leer el fichero confidencial de cuentas»

La **denegación de servicio** impide o inhibe el normal uso o gestión de servicios de comunicación. Este ataque puede tener un objetivo específico. Por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino concreto (por ejemplo, al servicio de vigilancia de seguridad). Otro tipo de denegación de servicio es la interrupción de un servidor o de toda una red, bien deshabilitando el servidor o sobrecargándolo con mensajes con objeto de degradar su rendimiento.

Los ataques activos presentan características opuestas a las de los ataques pasivos. Mientras que un ataque pasivo es difícil de detectar, existen medidas para impedir que tengan éxito. Por otro lado, es bastante difícil impedir ataques activos de forma absoluta, ya que para hacerlo se requeriría protección física permanente de todos los recursos y de todas las rutas de comunicación. En su lugar, el objetivo consiste en detectarlos y recuperarse de cualquier interrupción o retardo causados por ellos. Ya que la detección tiene un efecto disuasorio, también puede contribuir a la prevención.

21.2. PRIVACIDAD CON CIFRADO SIMÉTRICO

La técnica universal para proporcionar privacidad en los datos transmitidos es el cifrado simétrico. Esta sección examina primero los conceptos básicos del cifrado simétrico y sigue con una discusión sobre las dos técnicas de cifrado simétrico más importantes: el estándar de cifrado de datos (DES, *Data Encryption Standard*) y el estándar de cifrado avanzado (AES, *Advanced Encryption Standard*). Después se examinará la aplicación de estas técnicas para lograr la privacidad.

CIFRADO SIMÉTRICO

El cifrado simétrico, también denominado cifrado convencional o de clave única, era el único tipo de cifrado en uso antes de la introducción del cifrado de clave pública a finales de la década de los setenta. Innumerables individuos y grupos, desde Julio César, pasando por la fuerza alemana U-boat, hasta los actuales usuarios diplomáticos, militares y comerciales, han empleado el cifrado simétrico para la comunicación secreta. De los dos tipos de cifrado, es todavía el más utilizado.

Un esquema de cifrado simétrico tiene cinco ingredientes (*véase* Figura 21.1):

- **Texto nativo (*plaintext*):** es el mensaje original o datos que se proporcionan como entrada del algoritmo.
- **Algoritmo de cifrado:** el algoritmo de cifrado lleva a cabo varias sustituciones y transformaciones sobre el texto nativo.
- **Clave secreta:** la clave secreta es también una entrada del algoritmo de cifrado. Las sustituciones y transformaciones concretas realizadas por el algoritmo dependen de la clave.
- **Texto cifrado (*ciphertext*):** es el mensaje alterado que se produce como salida. Depende del texto nativo y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.
- **Algoritmo de descifrado:** es esencialmente el algoritmo de cifrado ejecutado a la inversa. Toma como entradas el texto cifrado y la clave secreta y produce como salida el texto nativo original.

Existen dos requisitos para la utilización segura del cifrado simétrico:

1. Se necesita un algoritmo de cifrado robusto. Como mínimo, es de desear que el algoritmo cumpla que aunque un oponente conozca el algoritmo y tenga acceso a uno o más textos cifrados, sea incapaz de descifrar el texto o averiguar la clave. Este requisito se suele enunciar de una forma más estricta: el oponente debería ser incapaz de descifrar el texto o descubrir la clave incluso si él o ella poseyera varios textos cifrados junto a sus correspondientes textos nativos.
2. El emisor y el receptor tienen que haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y conoce el algoritmo, toda comunicación que utilice esta clave puede ser leída.

Existen dos enfoque generales para atacar el esquema de cifrado simétrico. El primer ataque se conoce como **criptoanálisis**. Los ataques de criptoanálisis se basan en la naturaleza del algoritmo

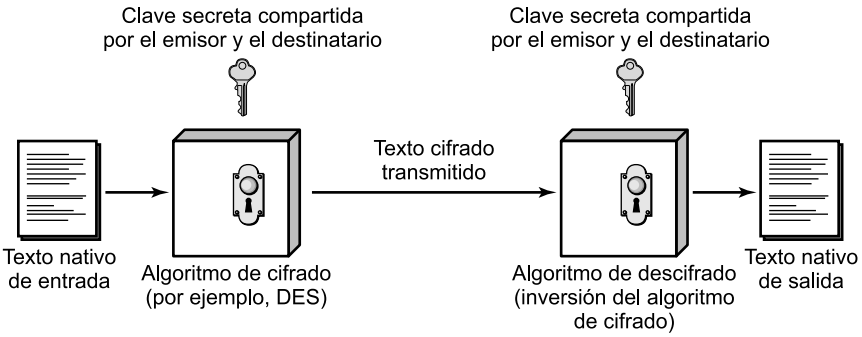


Figura 21.1. Modelo simplificado de cifrado simétrico.

junto a algún posible conocimiento de las características generales del texto nativo o incluso de algunos pares de texto nativo y cifrado. Este tipo de ataque explota las características del algoritmo para intentar deducir un texto nativo concreto o deducir la clave que se esté utilizando. Si el ataque tiene éxito en la deducción de la clave, el efecto es catastrófico: todos los mensajes cifrados con esa clave, pasados y futuros, están comprometidos.

El segundo método, conocido como ataque por **fuerza bruta**, consiste en probar cada posible clave sobre un fragmento de texto cifrado hasta que se obtenga una traducción inteligible de texto nativo. La Tabla 21.1 muestra la cantidad de tiempo que necesita este ataque frente a varias longitudes de clave. La tabla muestra los resultados para cada tamaño de clave, suponiendo que se tarda 1 μs en llevar a cabo un único descifrado, un orden de magnitud razonable para los computadores actuales. Con el uso de una masiva organización paralela de microprocesadores sería posible alcanzar tasas de procesamiento de varios órdenes de magnitud superiores. La última columna de la tabla considera los resultados de un sistema que pudiera procesar 1 millón de claves por microsegundo. Como se puede ver, a este nivel de rendimiento ya no se puede considerar segura en términos computacionales una clave de 56 bits.

Tabla 21.1. Tiempo promedio necesario para una búsqueda de clave exhaustiva

Tamaño de la clave (bits)	Número de claves alternativas	Tiempo necesario a 1 cifrado/μs	Tiempo necesario a 10^6 cifrados/μs
32	$2^{32} = 4{,}3 \times 10^9$	2^{31} μs = 35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1.142 años	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	2^{127} μs = $5{,}4 \times 10^{24}$ años	$5{,}4 \times 10^{18}$ años
168	$2^{168} = 3{,}7 \times 10^{50}$	2^{167} μs = $5{,}9 \times 10^{36}$ años	$5{,}9 \times 10^{30}$ años

ALGORITMOS DE CIFRADO

Los algoritmos de cifrado simétrico más comúnmente empleados son los cifradores de bloque. Un cifrador de bloque procesa una entrada de texto nativo en bloques de tamaño fijo y produce un bloque de texto cifrado de igual tamaño por cada bloque de texto nativo. Los dos algoritmos simétricos más importantes, ambos cifradores de bloque, son el estándar de cifrado de datos (DES) y el estándar avanzado de cifrado (AES).

El estándar de cifrado de datos (DES)

DES ha constituido el algoritmo de cifrado dominante desde su introducción en 1977. Sin embargo, dado que DES emplea sólo una clave de 56 bits, fue sólo una cuestión de tiempo que la velocidad de procesamiento computacional dejara a DES obsoleto. En 1998, la Fundación de la Frontera Electrónica (EFF, *Electronic Frontier Foundation*) anunció que había roto un reto de DES empleando una máquina de propósito específico para forzar DES, construida por menos de 250.000 dólares. El ataque duró menos de tres días. La EFF ha publicado una descripción detallada de la máquina, permitiendo que otros construyan su propio saboteador [EFF98]. Por supuesto, los precios del hardware continuarán cayendo al mismo tiempo que la velocidad de procesamiento irá aumentando, haciendo de DES un algoritmo inútil.

La vida de DES fue prolongada gracias al uso de triple DES (3DES), que supone la repetición del algoritmo básico DES tres veces, utilizando dos o tres claves únicas, para una longitud de clave de 112 o 168 bits.

El principal inconveniente de 3DES consiste en que el algoritmo por software es relativamente lento. Un inconveniente secundario es que tanto DES como 3DES utilizan un tamaño de bloque de 64 bits. Por razones de eficiencia y de seguridad, es deseable emplear bloques de mayor longitud.

Estándar de cifrado avanzado (AES)

A causa de las mencionadas deficiencias, 3DES no constituye un candidato razonable para su empleo a largo plazo. Como sustituto, el Instituto Nacional de Estándares y Tecnología (NIST, *National Institute of Standards and Technology*) publicó en 1997 una convocatoria de propuestas para un nuevo estándar de cifrado avanzado (AES, *Advanced Encryption Standard*), que debería poseer una robustez de seguridad igual o superior a la de 3DES y mejorar significativamente su eficiencia. Además de esos requisitos generales, NIST especificó que AES tenía que ser un cifrador de bloque simétrico con una longitud de bloque de 128 bits y admitir longitudes de claves de 128, 192 y 256 bits. Los criterios de evaluación incluían seguridad, eficiencia computacional, requerimientos de memoria, disponibilidad de software y hardware y flexibilidad. En 2001 se publicó AES como un estándar federal de procesamiento de información (FIPS 197, *Federal Information Processing Standard*).

En la descripción de esta sección suponemos una longitud de clave de 128 bits, que será probablemente una de las más comúnmente implementadas.

La Figura 21.2 muestra la estructura global de AES. La entrada de los algoritmos de cifrado y descifrado es un bloque de 128 bits. En FIPS 197, este bloque se representa mediante una matriz cuadrada de bytes. Este bloque se copia en el vector **estado**, que se modifica en cada etapa del cifrado o descifrado. Tras la etapa final, se copia el contenido de **estado** en una matriz de salida. De forma similar, la clave de 128 bits se representa como una matriz cuadrada de bytes. Esta clave se expande en un vector de palabras de planificación de clave. Cada palabra consta de cuatro bytes y la planificación total de la clave ocupa 44 palabras para una clave de 128 bits. Dentro de la matriz, los bytes se ordenan por columnas. Así, por ejemplo, los primeros cuatro bytes de un texto nativo de 128 bits de entrada al cifrador ocupan la primera columna de la matriz **dentro**, los siguientes cuatro bytes ocupan la segunda columna y así sucesivamente. De forma similar, los primeros cuatro bytes de la clave expandida que forman una palabra ocupan la primera columna de la matriz **w**.

Los comentarios siguientes pueden aclarar el funcionamiento de AES:

1. La clave que se proporciona como entrada se expande en un vector de cuarenta y cuatro palabras de 32 bits, **w**[*i*]. Cuatro palabras distintas (128 bits) sirven como clave de ronda para cada vuelta.
2. Se emplean cuatro etapas diferentes: una de permutación y tres de sustitución. Consisten en:
   - **Sustituir bytes:** en esta etapa se utiliza una tabla, llamada caja-S[1] (*S-box*) para efectuar una sustitución del bloque byte a byte.
   - **Desplazar filas:** esta etapa efectúa una permutación simple fila a fila.

[1] El término *caja-S* (*S-box*), o caja de sustitución, se emplea comúnmente en la descripción de cifradores simétricos para referirse a una tabla utilizada para un mecanismo de sustitución del tipo consulta en tabla.

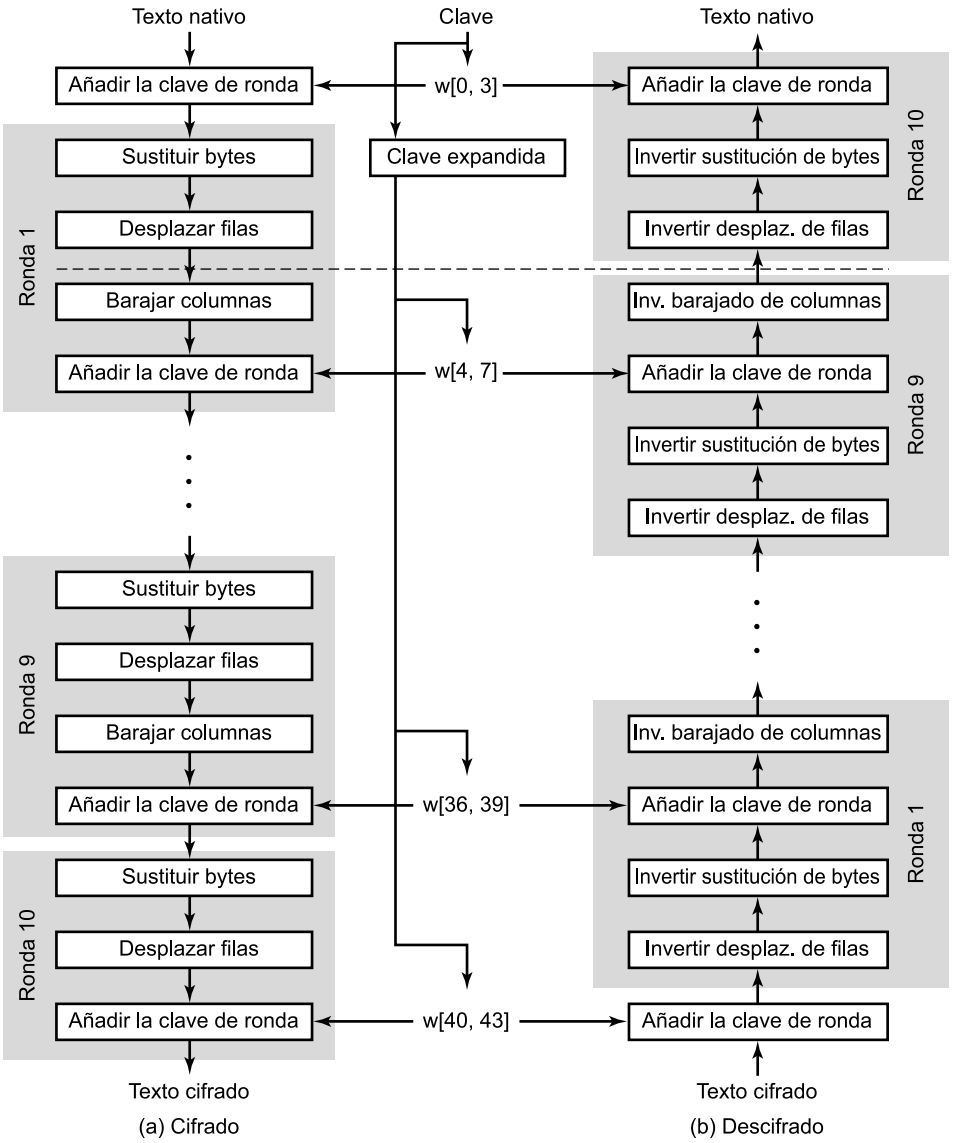


Figura 21.2. Cifrado y descifrado AES.

- **Barajar columnas:** se lleva a cabo una sustitución que modifica cada byte de una columna como función de todos los bytes de la misma.
- **Añadir clave de ronda:** se efectúa en esta etapa una operación XOR binaria del bloque actual con una porción de la clave expandida.

3. La estructura es bastante sencilla. Para el cifrado y descifrado, el cifrador comienza con una etapa de adición de la clave de ronda, seguida de nueve rondas que incluyen cada una cuatro etapas, seguidas por una décima ronda de tres etapas. La Figura 21.3 representa la estructura de una ronda de cifrado completa.

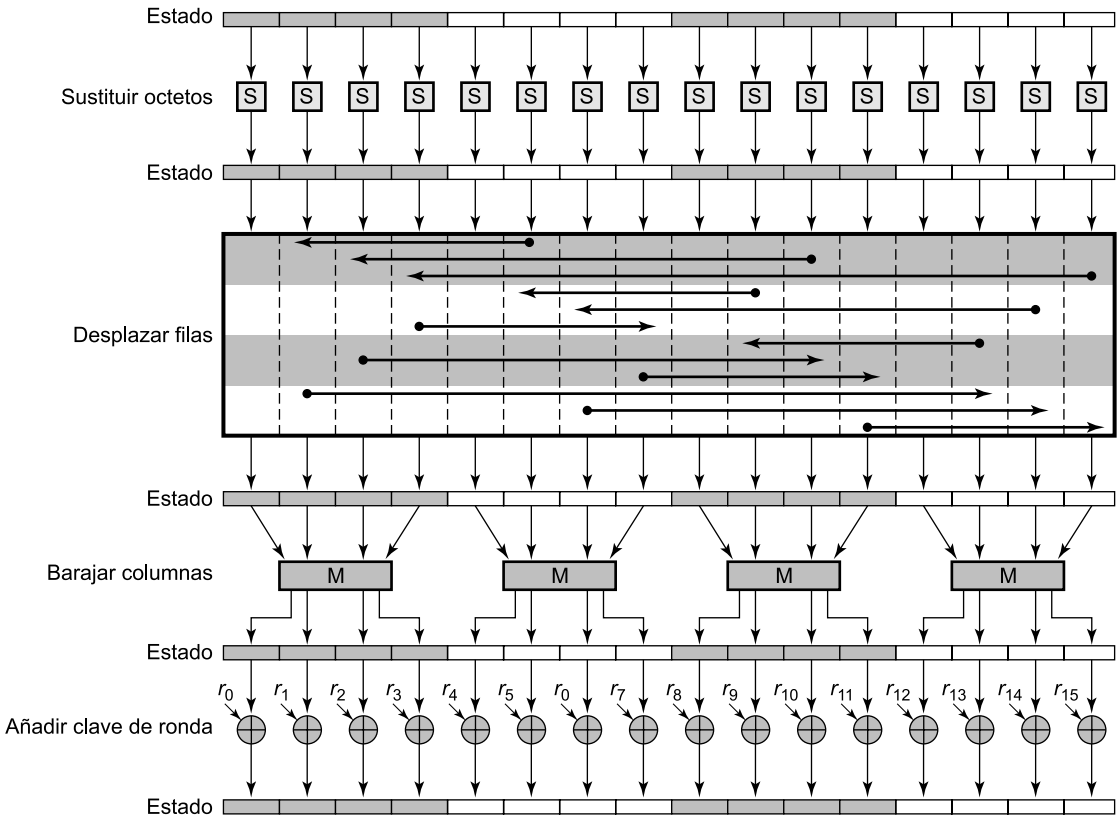


Figura 21.3. Ronda de cifrado AES.

4. Sólo la etapa de adición de la clave de ronda hace uso de la clave. Por esta razón, el cifrado comienza y termina con una etapa de adición de la clave de ronda. Cualquier otra etapa, aplicada al principio o al final, es reversible sin necesidad de conocer la clave y por eso no añadiría seguridad.

5. La etapa de adición de la clave de ronda no sería excepcional en sí misma. Las otras tres etapas juntas desordenan los bits, pero no proporcionarían seguridad por ellos mismos, ya que no utilizan la clave. Podemos ver el cifrado como una sucesión de operaciones alternas de cifrado XOR de un bloque (adición de la clave de ronda), seguido por el barajado del bloque (las otras tres etapas), seguido de cifrado XOR y así sucesivamente. Este esquema es eficiente y muy seguro.

6. Cada etapa es fácilmente reversible. Para las etapas de sustitución de bytes, desplazamiento de filas y adición de la clave de ronda se utiliza una función inversa en el algoritmo de descifrado. Para la etapa de adición de la clave de ronda, la inversión se obtiene mediante la operación XOR de la misma clave de ronda sobre el bloque, debido a que $A \oplus A \oplus B = B$.

7. Como la mayoría de los cifradores de bloque, el algoritmo de descifrado hace uso de la clave expandida en orden inverso. Sin embargo, el algoritmo de descifrado no es idéntico al de cifrado. Esto es consecuencia de la particular estructura de AES.

8. Una vez que se ha establecido que las cuatro etapas son reversibles, es fácil verificar que el descifrado recupera efectivamente el texto nativo. La Figura 21.2 traza el cifrado y el descifrado verticalmente en sentidos opuestos. En cada punto horizontal, (por ejemplo, la línea discontinua de la figura), la variable **estado** es la misma para el cifrado y el descifrado.
9. La ronda final del cifrado y el descifrado consta sólo de tres etapas. De nuevo, es consecuencia de la particular estructura de AES, siendo necesario para que el cifrado sea reversible.

LOCALIZACIÓN DE LOS DISPOSITIVOS DE CIFRADO

La aproximación más efectiva y común para enfrentarse a los ataques a la seguridad de la red es el cifrado. Si se utiliza, entonces necesitamos decidir qué vamos a cifrar y dónde se va a situar el equipo de cifrado. Como indica la Figura 21.4, existen dos alternativas fundamentales: el cifrado de enlace y el cifrado extremo a extremo.

En el cifrado de enlace, cada enlace de comunicaciones vulnerable se equipa con un dispositivo de cifrado en ambos extremos. Así se protege todo el tráfico que atraviese los enlaces de comunicaciones. Aunque esto requiere gran número de dispositivos de cifrado en redes amplias, este esquema proporciona un alto nivel de seguridad. Una desventaja de esta aproximación consiste en que el mensaje debe ser descifrado cada vez que entra en un conmutador de paquetes. Esto se debe a que el conmutador debe leer la dirección (número de circuito virtual) de la cabecera del paquete para encaminarlo. Así, el mensaje es vulnerable en cada conmutador. Si se trata de una red de conmutación de paquetes pública, el usuario no tiene control sobre la seguridad de los nodos.

Con un cifrado extremo a extremo, el proceso de cifrado se efectúa en los dos sistemas finales. La estación o terminal origen cifra los datos, que en forma cifrada se transmiten sin modificación a través de la red hasta la estación o terminal destino. El destino comparte una clave con el origen y

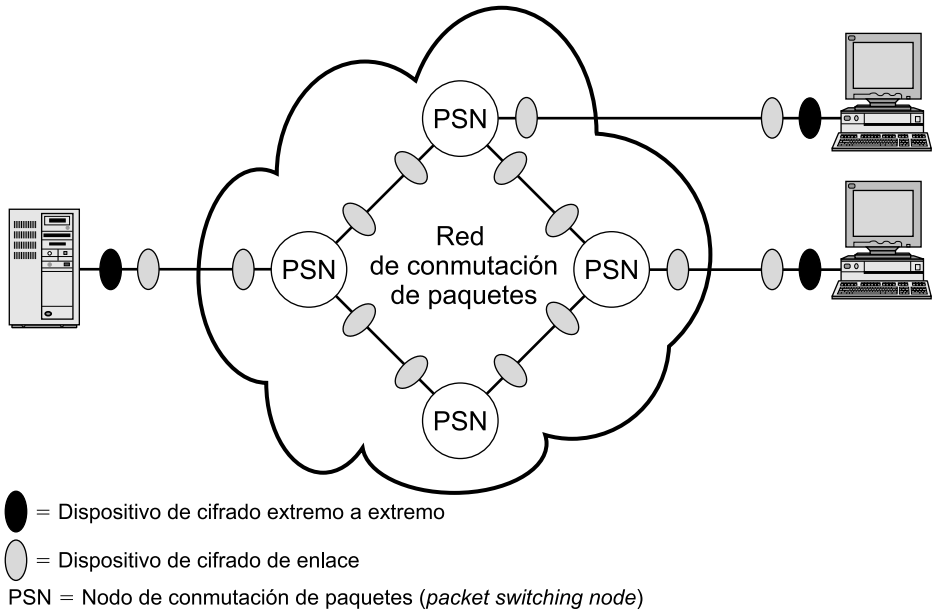


Figura 21.4. Cifrado a través de una red de conmutación de paquetes.

es así capaz de descifrar los datos. Esta técnica parece proteger la transmisión contra ataques en los enlaces o conmutadores de la red. Sin embargo, existe aún un punto débil.

Considere la siguiente situación: un computador se conecta a una red de conmutación de paquetes X.25, establece un circuito virtual a otro computador y se prepara para transferir los datos al otro computador utilizando un cifrado extremo a extremo. Los datos se transmiten sobre esa red en forma de paquetes que constan de una cabecera y algunos datos de usuario. ¿Qué parte de cada paquete cifrará el computador? Supongamos que el computador cifra el paquete entero, incluyendo la cabecera. Esto no funcionará ya que, recuerde, sólo el otro computador puede realizar el descifrado. El nodo de conmutación de paquetes recibirá un paquete cifrado y no será capaz de leer la cabecera. Por tanto, no será capaz de encaminar el paquete. De esto se deduce que el computador sólo puede cifrar la parte de datos de usuario del paquete y debe dejar la parte de la cabecera intacta, para que la red pueda leerla.

De esta manera, con el cifrado extremo a extremo, los datos de usuario están seguros. Sin embargo, el patrón de tráfico no lo está, ya que las cabeceras de los paquetes se transmiten sin cifrar. Para lograr un mayor grado de seguridad, se necesitan el cifrado del enlace y el extremo a extremo, como se muestra en la Figura 21.4.

Para resumir, cuando se emplean ambas alternativas, el computador cifra la parte de datos de usuario usando una clave de cifrado extremo a extremo. Después se cifra el paquete completo usando una clave de cifrado de enlace. Conforme el paquete recorre la red, cada conmutador descifra el paquete utilizando una clave de cifrado de enlace para leer la cabecera y luego cifrar de nuevo el paquete entero para enviarlo por el siguiente enlace. Ahora el paquete entero está seguro, excepto durante el tiempo en el que el paquete está realmente en la memoria de un conmutador de paquetes, ya que la cabecera está desprotegida durante dicho intervalo.

DISTRIBUCIÓN DE CLAVES

Para que funcione el cifrado simétrico, las dos partes que realizarán un intercambio seguro de datos deben tener la misma clave y ésta debe protegerse para que no sea accesible por otros. Es más, es normalmente deseable realizar cambios frecuentes de la clave para limitar la cantidad de datos comprometidos si un atacante averiguara la clave. Por tanto, la fortaleza de cualquier sistema de cifrado reside en la técnica de distribución de claves empleada, un término que se refiere a los medios para distribuir una clave a las dos partes que deseen intercambiar datos, impidiendo que otros la vean. La distribución de claves se puede lograr de varias formas. Para dos partes A y B:

1. A podría seleccionar una clave y entregársela físicamente a B.
2. Una tercera parte podría seleccionar la clave y entregársela físicamente a B y A.
3. Si A y B han utilizado previa y recientemente una clave, una de las partes podría transmitir a la otra la nueva clave cifrada con la antigua clave.
4. Si A y B tienen cada uno una conexión cifrada con una tercera parte C, C podría entregar a B y A una clave a través de los enlaces cifrados.

Las opciones 1 y 2 exigen una entrega manual de la clave. Éste es un requisito razonable para el cifrado de enlace, ya que cada dispositivo de cifrado de enlace va sólo a intercambiar datos con su pareja del otro extremo de enlace. Sin embargo, para el cifrado extremo a extremo, la entrega manual es complicada. En un sistema distribuido, cualquier terminal o computador dado puede necesitar efectuar intercambios con muchos otros terminales o computadores a lo largo del tiempo. Así,

cada dispositivo necesita varias claves proporcionadas dinámicamente. El problema es especialmente difícil en sistemas distribuidos de área extensa.

La opción 3 constituye una posibilidad válida tanto para el cifrado de enlace como para el cifrado extremo a extremo, pero si un atacante tiene éxito consiguiendo una clave, entonces todas las claves posteriores son reveladas. Incluso si se cambian frecuentemente las claves de cifrado de enlace, dichos cambios deben realizarse manualmente. Por tanto, se prefiere la opción 4 para el cifrado extremo a extremo.

La Figura 21.5 muestra una implementación de la opción 4 para el cifrado extremo a extremo. En la figura se ha ignorado el cifrado de enlace, que se puede incorporar o no según se requiera. En este esquema se identifican dos clases de claves:

- **Clave de sesión:** cuando dos sistemas finales (computadores, terminales, etc.) desean comunicarse, establecen una conexión lógica (por ejemplo: circuitos virtuales). Durante la duración de la conexión lógica, todos los datos de usuario se cifran con una clave de sesión de un solo uso. Al terminar la sesión o la conexión, la clave de sesión se destruye.
- **Clave permanente:** es una clave que se emplea entre entidades para la distribución de claves de sesión.

La configuración consta de los siguientes elementos:

- **Centro de distribución de claves (KDC, *Key Distribution Center*):** el centro de distribución de claves determina a qué sistemas se les permite comunicarse entre ellos. Cuando a dos sistemas se les concede el permiso para establecer una conexión, el centro de distribución de claves proporciona una clave de sesión para esa conexión.
- **Módulo de servicio de seguridad (SSM, *Security Service Module*):** este módulo, que puede componerse de funciones de una capa de protocolo, lleva a cabo el cifrado extremo a extremo y obtiene las claves de sesión en nombre de los usuarios.

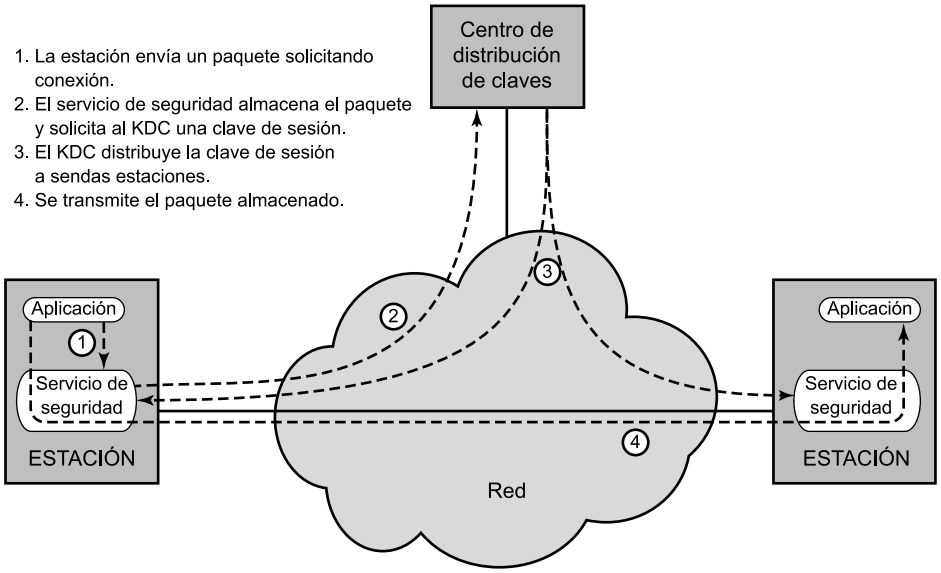


Figura 21.5. Distribución automática de claves para protocolos orientados a conexión.

Los pasos necesarios para establecer una conexión se muestran en la figura. Cuando una estación desea establecer una conexión con otra estación, transmite un paquete de solicitud de conexión (paso 1). El SSM guarda ese paquete y solicita al KDC permiso para establecer la conexión (paso 2). La comunicación entre el SSM y el KDC está cifrada utilizando una clave maestra compartida sólo por este SSM y el KDC. Si el KDC aprueba la solicitud de conexión, genera una clave de sesión y se la entrega a los dos SSM correspondientes, utilizando una clave permanente única para cada SSM (paso 3). El SSM solicitante puede ahora liberar el paquete de solicitud de conexión y se establece así una conexión entre los dos sistemas finales (paso 4). Todos los datos de usuario intercambiados entre los dos sistemas finales son cifrados por sus respectivos SSM empleando la clave de sesión de un sólo uso.

La estrategia de la distribución automática de claves proporciona las características de flexibilidad y dinamismo necesarias para permitir a varios usuarios de terminales acceder a distintas estaciones y a las estaciones les permite intercambiar datos con cada una de las otras.

Otra aproximación para la distribución de claves se basa en el cifrado de clave pública, que será analizada en la Sección 21.4.

RELLENO DE TRÁFICO

Hemos mencionado que, en algunos casos, a los usuarios les preocupa la seguridad en casos de análisis de tráfico. Con el uso de cifrado de enlace, las cabeceras de los paquetes se cifran, reduciendo la posibilidad de efectuar análisis de tráfico. No obstante, es todavía posible en esas circunstancias que un atacante calcule la cantidad de tráfico en una red y observe la cantidad de tráfico que entra y que sale de cada sistema final. Una contramedida efectiva a este ataque es el relleno de tráfico.

El relleno de tráfico es una función que produce continuamente texto cifrado, incluso en ausencia de texto nativo. Genera un flujo de datos aleatorio continuo. Cuando hay disponible texto nativo, se cifra y se transmite. Cuando el texto nativo no está presente, los datos aleatorios son cifrados y transmitidos. Esto imposibilita a un atacante distinguir entre el flujo de datos verdaderos y el ruido y, por tanto, le resulta imposible deducir la cantidad de tráfico.

21.3. AUTENTICACIÓN DE MENSAJES Y FUNCIONES DE DISPERSIÓN (*HASH*)

El cifrado protege contra los ataques pasivos (escuchas). Proteger contra ataques activos (falsificación de datos y transacciones) constituye un requisito diferente. La protección contra tales ataques se conoce como autenticación de mensajes.

ALTERNATIVAS PARA LA AUTENTICACIÓN DE MENSAJES

Un mensaje, fichero, documento u otro conjunto de datos se dice estar autenticado cuando es genuino y proviene del origen pretendido. La autenticación de mensajes es un procedimiento que permite a las partes que se comunican verificar que los mensajes recibidos son auténticos. Los dos aspectos importantes son verificar que el contenido del mensaje no se ha alterado y que el origen es auténtico. También podemos desear verificar la temporización de un mensaje (que no haya sido artificialmente retrasado y retransmitido) y verificar su secuencia relativa a los otros mensajes que se transmitan entre las dos partes.

Autenticación mediante cifrado simétrico

Es posible llevar a cabo la autenticación simplemente mediante el uso del cifrado simétrico. Si suponemos que solamente el emisor y el receptor comparten una clave (que es lo que debe ocurrir), entonces solamente el emisor genuino sería capaz de cifrar un mensaje satisfactoriamente para el otro participante. Es más, si el mensaje incluye un código de detección de errores y un número de secuencia, se le asegura al receptor que no se han efectuado modificaciones y que la secuencia es la adecuada. Si el mensaje incluye también una marca de tiempo, el receptor tiene la seguridad de que el mensaje no se ha retrasado más de lo normalmente esperado en el tránsito por la red.

Autenticación de mensajes sin cifrado de mensajes

En esta sección, examinaremos varias estrategias para autenticar mensajes que no se basan en el cifrado. En todas estas aproximaciones se genera una etiqueta de autenticación que se incorpora al mensaje para su transmisión. El mensaje mismo no está cifrado y se puede leer en el destino independientemente de la función de autenticación del mismo.

Ya que las técnicas descritas en esta sección no cifran el mensaje, al mensaje no se le proporciona privacidad. Dado que el cifrado simétrico proporciona autenticación y, dado que se utiliza ampliamente en productos existentes, ¿por qué no utilizar esta aproximación, que proporciona tanto privacidad como autenticación? En [DAVI89] se sugieren tres situaciones en las que es preferible la autenticación sin privacidad:

1. Existen varias aplicaciones en las que el mismo mensaje se difunde a diferentes destinos. Por ejemplo, una notificación a los usuarios de que la red no está disponible en ese momento o una señal de alarma en un centro de control. Es más barato y más fiable tener solamente un destino para monitorizar la autenticación. De este modo, el mensaje debe difundirse en texto nativo con una etiqueta de autenticación del mensaje asociada. El sistema responsable lleva a cabo la autenticación. Si se detecta una violación de la autenticidad, se alerta a los otros sistemas destino mediante una alarma general.
2. Otro posible escenario consiste en un intercambio en el que una de las partes soporta una carga muy elevada y no tiene tiempo de descifrar todos los mensajes que recibe. La autenticación se efectúa de forma selectiva, eligiendo mensajes de forma aleatoria para realizar las comprobaciones.
3. La autenticación de un programa de computador en texto nativo es un servicio interesante. El programa se puede ejecutar sin tener que descifrarlo cada vez, lo que supondría un derroche de recursos de procesamiento. Sin embargo, si una etiqueta de autenticación de mensaje fuera incorporada al programa, se podría comprobar ésta siempre que se necesitara tener certeza de la integridad del programa.

Así, hay lugar para el cifrado y la autenticación a la hora de satisfacer requisitos de seguridad.

Código de autenticación de mensajes

Una técnica de autenticación supone el uso de una clave secreta para generar un pequeño bloque de datos, conocido como código de autenticación del mensaje (MAC, *Message Authentication Code*), e incorporarlo al mismo. Esta técnica supone que dos partes comunicantes, digamos A y B, comparten una clave secreta común K_{AB}. Cuando A tiene un mensaje M que enviar a B, calcula el

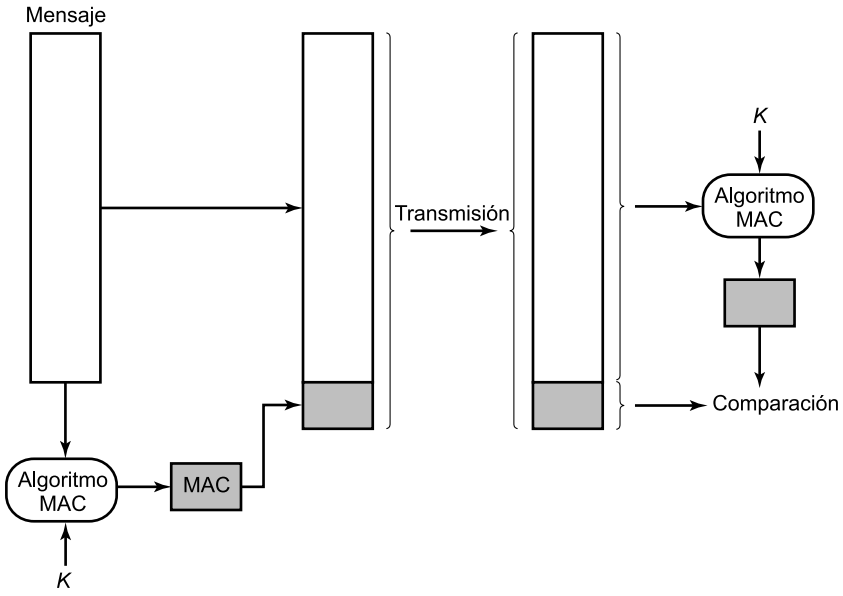


Figura 21.6. Autenticación de mensaje mediante un código de autenticación del mensaje.

código de autenticación del mensaje como una función del mensaje y la clave: $MAC_M = F(K_{AB}, M)$. Luego se transmite el mensaje más el código al destinatario deseado. El destinatario realiza los mismos cálculos sobre el mensaje recibido, utilizando la misma clave secreta, para generar un nuevo código de autenticación del mensaje. El código recibido se compara con el código calculado (*véase* Figura 21.6). Si suponemos que sólo el emisor y el receptor conocen la identidad de la clave secreta y si el código recibido coincide con el calculado, entonces:

1. El receptor está seguro de que el mensaje no ha sido alterado. Si un atacante altera el mensaje pero no el código, el código calculado en el receptor diferirá del código recibido. Ya que se supone que el atacante no conoce la clave secreta, éste no podrá modificar el código para que corresponda con la alteración del mensaje.

2. El receptor está seguro de que el mensaje es del emisor pretendido. Ya que nadie más conoce la clave secreta, nadie más podría preparar un mensaje con el código apropiado.

3. Si el mensaje incluye un número de secuencia (como los que se utilizan en X.25, HDLC y TCP), entonces el receptor puede estar seguro de la secuencia adecuada, ya que un atacante no puede alterar el número de secuencia satisfactoriamente.

Se pueden utilizar diversos algoritmos para generar el código. El Departamento Nacional de Estándares recomienda en su publicación «Modos de funcionamiento de DES» el uso del algoritmo DES. Se utiliza DES para generar una versión cifrada del mensaje y los últimos bits del texto cifrado se utilizan como código. Generalmente se utilizan códigos de 16 o 32 bits.

El proceso descrito es similar al del cifrado. Una de las diferencias consiste en que el algoritmo de autenticación no necesita ser reversible, al contrario que en el caso del descifrado. Resulta que, debido a las propiedades matemáticas de la función de autenticación, ésta es menos vulnerable a ser rota que el cifrado.

Función de dispersión de un solo sentido

Una variación del código de autenticación de mensajes al que se le ha prestado mucha atención recientemente es la función de dispersión de un solo sentido (*one-way hash function*). Como ocurre con el código de autenticación de mensajes, una función de dispersión acepta un mensaje M de longitud variable como entrada y produce un resumen del mensaje de longitud fija H(M) como salida. A diferencia del MAC, la función de dispersión no toma como entrada una clave secreta. Para autenticar un mensaje se envía junto a él el resumen del mensaje de forma que el resumen sea auténtico.

La Figura 21.7 muestra tres formas en las que se puede autenticar un mensaje. El resumen del mensaje se puede cifrar mediante cifrado simétrico (parte a). Si se supone que sólo el emisor y el receptor comparten la clave, se asegura la autenticación. El resumen del mensaje también se puede

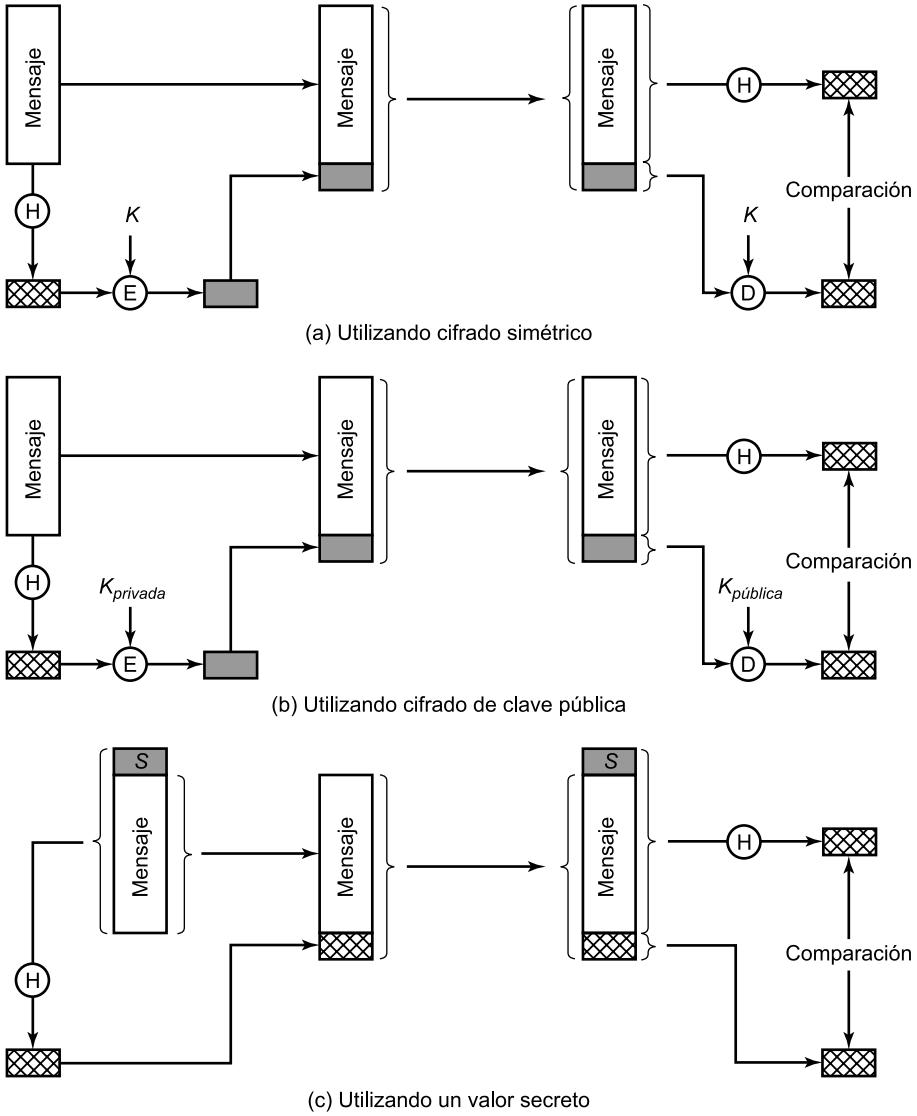


Figura 21.7. Autenticación de un mensaje mediante una función de dispersión de un solo sentido.

cifrar utilizando cifrado de clave pública (parte b), como se explica en la Sección 21.4. La estrategia de clave pública tiene dos ventajas: proporciona una firma digital, así como la autenticación de los mensajes, y no requiere distribuir claves a las partes que se comuniquen.

Estas dos aproximaciones tienen la ventaja de requerir menos cálculo con respecto a los esquemas que cifran el mensaje completo. No obstante, ha habido interés en desarrollar una técnica que evite el cifrado del conjunto. En [TSUD92] se apuntan algunas razones de este interés:

- El software de cifrado es muy lento. Aunque la cantidad de datos que se ha de cifrar por mensaje sea pequeña, puede haber un flujo constante de mensajes desde y hacia el sistema.
- El coste del hardware de cifrado no es despreciable. Hay disponibles implementaciones del algoritmo DES en chips de bajo coste, pero este coste puede incrementarse bastante si todos los nodos de una red tienen que disponer de esta capacidad.
- El hardware de cifrado está optimizado para grandes tamaños de datos. Para pequeños bloques de datos, se emplea una alta proporción del tiempo en la sobrecarga de inicialización e invocación.
- Los algoritmos de cifrado pueden estar protegidos por patentes. Algunos algoritmos de cifrado, como el algoritmo de clave pública RSA, están patentados y necesitan licencia, lo que aumenta el coste.
- Los algoritmos de cifrado pueden estar sujetos al control de exportación.

La Figura 21.7c muestra una técnica que utiliza una función de dispersión, pero no cifrado, para la autenticación del mensaje. Esta técnica supone que las dos partes que se comunican, digamos A y B, comparten un valor secreto común S_{AB}. Cuando A tiene un mensaje que enviar a B, calcula la función de dispersión sobre la concatenación de la clave secreta y el mensaje: $MD_M = H(S_{AB} \| M)$[2]. Entonces A envía $[M \| MD_M]$ a B. B puede recalcular $H(S_{AB} \| M)$ y verificar MD_M, ya que también posee S_{AB}. Ya que el valor secreto no se envía, para un atacante es imposible modificar un mensaje interceptado. Mientras el valor secreto se mantenga oculto, también le será imposible a un atacante generar un mensaje falso.

Esta tercera técnica, consistente en emplear un valor secreto común, es la que ha adoptado IP para implementar seguridad. También ha sido especificada para SNMPv3, discutido en el Capítulo 22.

FUNCIONES DE DISPERSIÓN SEGURAS

La función de dispersión de un solo sentido, o función de dispersión segura, es importante no sólo para la autenticación de mensajes, sino también para las firmas digitales. En esta sección comenzaremos discutiendo los requisitos de una función de dispersión segura. Después examinaremos una de las funciones de dispersión más relevantes, SHA-1.

Requisitos para una función de dispersión segura

El objetivo de una función de dispersión es producir una «huella dactilar» de un fichero, mensaje, u otro bloque de datos. Para que sea útil para la autenticación, una función de dispersión H debe cumplir las propiedades siguientes:

[2] «||» indica concatenación.

1. H puede ser aplicada a un bloque de datos de cualquier tamaño.
2. H produce una salida de longitud fija.
3. Para cualquier x dado, es relativamente fácil calcular $H(x)$, haciendo factibles las implementaciones hardware y software.
4. Para cualquier código h, por limitaciones computacionales, es inviable encontrar un x tal que $H(x) = h$.
5. Para cualquier bloque x, por limitaciones computacionales, es inviable encontrar un $y \neq x$ para el que $H(y) = H(x)$.
6. Por limitaciones computacionales, es impracticable encontrar una pareja (x, y) tal que $H(x) = H(y)$.

Las tres primeras propiedades son requisitos para la aplicación práctica de una función de dispersión en la autenticación de mensajes.

La cuarta propiedad es la propiedad de «un solo sentido»: es fácil generar un código dado un mensaje, pero virtualmente imposible generar un mensaje a partir de un código. Esta propiedad es importante si la técnica de autenticación supone el uso de un valor secreto (*véase* Figura 21.7c). El valor secreto no se envía. Sin embargo, si la función de dispersión no es de un solo sentido, un atacante puede descubrir fácilmente el valor secreto. Si el atacante puede observar o interceptar una transmisión, obtendrá el mensaje M y el código de dispersión $MD_M = H(S_{AB} \| M)$. El atacante entonces invierte la función de dispersión para obtener $S_{AB} \| M = H^{-1}(MD_M)$. Dado que el atacante tiene ahora M y $[S_{AB} \| M]$, es una cuestión trivial obtener S_{AB}.

La quinta propiedad garantiza que no se pueda encontrar un mensaje alternativo que produzca el mismo valor de resumen que un mensaje dado. Esto impide la falsificación cuando se utiliza un código de dispersión cifrado (*véanse* Figura 21.7a y 21.7b). Si no se cumpliese esta propiedad, un atacante sería capaz de realizar la secuencia siguiente: en primer lugar, observar o interceptar un mensaje más su código de dispersión cifrado; en segundo lugar, generar un código de dispersión no cifrado a partir del mensaje; por último, generar un mensaje alternativo con el mismo código de dispersión.

A una función de dispersión que satisfaga las cinco primeras propiedades de la lista anterior se la conoce como función de dispersión débil. Si satisface también la sexta propiedad, entonces se la conoce como función de dispersión robusta. La sexta propiedad protege contra una clase de ataque sofisticado conocida como ataque del cumpleaños[3].

Además de proporcionar autenticación, un resumen de mensaje proporciona también integridad de los datos, ya que realiza la misma función que una secuencia de comprobación de trama: si algún bit es modificado accidentalmente en el tránsito, el resumen del mensaje será erróneo.

LA FUNCIÓN DE DISPERSIÓN SEGURA SHA-1

El algoritmo de dispersión segura (SHA, *Secure Hash Algorithm*) fue desarrollado por el NIST y publicado como estándar federal para el procesamiento de la información (FIPS 180) en 1993. En 1995 se publicó una versión revisada denominada FIPS 180-1, conocida generalmente como SHA-1.

[3] *Véase* [STAL03] para un estudio sobre el ataque del cumpleaños.

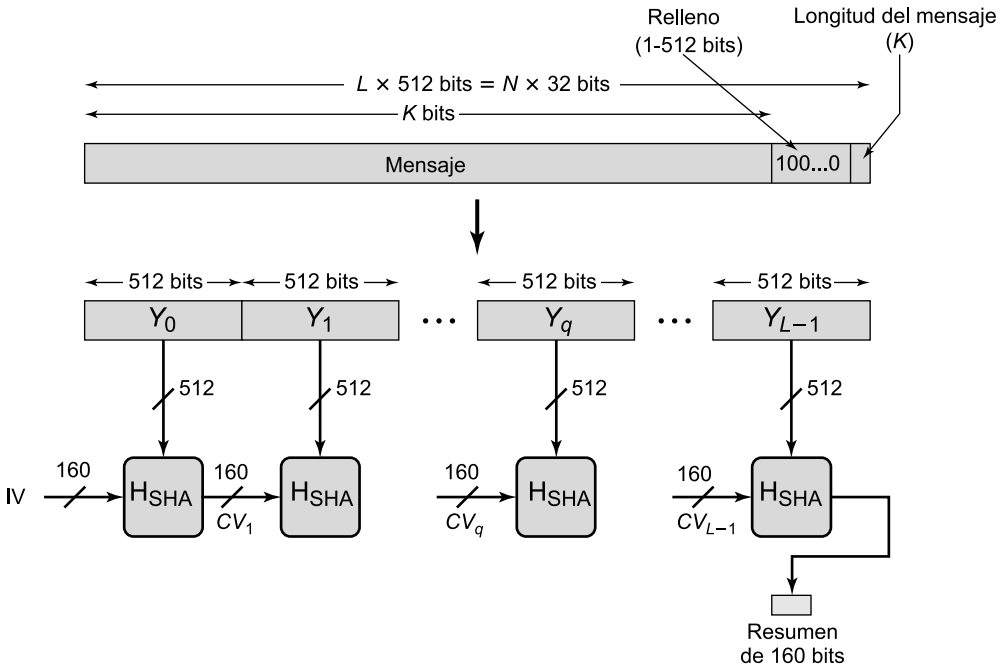


Figura 21.8. Generación del resumen de un mensaje mediante SHA-1.

El algoritmo toma como entrada un mensaje con una longitud máxima de 2^{64} bits y produce un resumen de mensaje de 160 bits. La entrada se procesa en bloques de 512 bits. La Figura 21.8 representa el procesamiento general de un mensaje para producir un resumen. El procesamiento consta de los siguientes pasos:

Paso 1: Añadir bits de relleno. Se completa el mensaje de forma que su longitud sea congruente con 448 módulo 512 (longitud = 448 mod 512). Es decir, la longitud del mensaje completado es 64 bits menor que un múltiplo de 512 bits. Siempre se incorpora el relleno, incluso si el mensaje tiene ya la longitud deseada. Así, el número de bits de relleno se encuentra en el rango de 1 a 512. El relleno se compone de un único bit con valor 1, seguido por el apropiado número de bits con valor cero.

Paso 2: Añadir longitud. Se añade al mensaje un bloque de 64 bits. Este bloque se trata como un entero de 64 bits sin signo (el byte más significativo primero) y contiene la longitud del mensaje original (antes de incorporar el relleno). La inclusión de un valor de longitud hace más difícil un tipo de ataque conocido como el ataque por relleno [TSUD92].

Como resultado de los dos primeros pasos se produce un mensaje cuya longitud es un múltiplo entero de 512 bits. En la Figura 21.8, el mensaje expandido se representa como una secuencia de bloques de 512 bits Y_0, Y_1, ..., Y_{L-1}, de manera que la longitud total del mensaje extendido es de $L \times 512$ bits. De forma equivalente, el resultado es un múltiplo de 16 palabras de 32 bits.

Paso 3: Inicializar la memoria temporal de MD. Se utiliza una memoria temporal de 160 bits para almacenar los resultados intermedios y finales de la función de dispersión.

Paso 4: Procesar el mensaje en bloques de 512 bits (palabras de 16 bits). El corazón del algoritmo es un módulo que consta de 4 rondas de procesamiento de 20 pasos cada uno. Las

cuatro rondas tienen una estructura similar, pero cada una utiliza una función lógica primitiva diferente. Cada ronda toma como entrada el bloque de 512 bits que se esté procesando (Y_q) y el valor de la memoria temporal de 160 bits, actualizando el contenido de la memoria temporal.

Paso 5: Producir la salida. Tras procesar los L bloques de 512 bits, la salida de la etapa L-ésima es el resumen de 160 bits del mensaje.

El algoritmo SHA-1 tiene la propiedad de que cada bit del código de dispersión es una función de cada bit de la entrada. El algoritmo produce resultados bien barajados. Es decir, es improbable que dos mensajes seleccionados de forma aleatoria tengan el mismo código de dispersión, incluso aunque manifiesten regularidades similares. A menos que exista alguna debilidad oculta en SHA-1, lo cual no ha sido publicado hasta ahora, la dificultad de que aparezcan dos mensajes con el mismo resumen de mensaje es del orden de 2^{80} operaciones, mientras que la dificultad de encontrar un mensaje con un resumen dado es del orden de 2^{160} operaciones.

21.4. CIFRADO DE CLAVE PÚBLICA Y FIRMAS DIGITALES

El cifrado de clave pública tiene la misma importancia que el cifrado simétrico, empleándose en la autenticación de mensajes y distribución de claves. Esta sección examina primero los conceptos básicos del cifrado de clave pública, seguido de una discusión sobre las firmas digitales. A continuación analizaremos el algoritmo de clave pública más utilizado: RSA. Después examinaremos el problema de la distribución de claves.

CIFRADO DE CLAVE PÚBLICA

El cifrado de clave pública, propuesto públicamente por primera vez por Diffie y Hellman en 1976 [DIFF76], es el primer avance realmente revolucionario en cuanto algoritmos de cifrado en, literalmente, miles de años. Y esto es debido a que el algoritmo de clave pública se basa en funciones matemáticas en lugar de en operaciones simples sobre patrones de bits. Pero más importante aún, la criptografía de clave pública es asimétrica, suponiendo el uso de dos claves diferentes, en contraste con el cifrado simétrico convencional, que sólo utiliza una. El uso de dos claves tiene profundas consecuencias en las áreas de privacidad, distribución de claves y autenticación.

Antes de proseguir, debemos mencionar varios conceptos erróneos comunes relacionados con el cifrado de clave pública. Uno de ellos es que el cifrado de clave pública es más seguro frente a criptoanálisis que el cifrado simétrico. En realidad, la seguridad de cualquier esquema de cifrado depende de (1) la longitud de la clave y (2) el esfuerzo computacional que requiere romper un cifrado. No hay nada en principio del cifrado simétrico o de clave pública que haga a uno superior respecto al otro desde el punto de vista de su resistencia frente al criptoanálisis. Un segundo malentendido es que el cifrado de clave pública es una técnica de propósito general que ha dejado obsoleto el cifrado simétrico. Por el contrario, a causa de la sobrecarga computacional de los esquemas de cifrado de clave pública actuales, no parece previsible que se abandone el cifrado simétrico. Finalmente, existe una concepción errónea de que la distribución de claves es trivial cuando se utiliza cifrado de clave pública, comparado con la engorrosa negociación que se requiere con los centros de distribución de claves en el cifrado simétrico. De hecho, se necesita algún tipo de protocolo, a menudo implicando a un agente central, y los procedimientos implicados no son más simples ni más eficientes que los que se requieren para el cifrado simétrico.

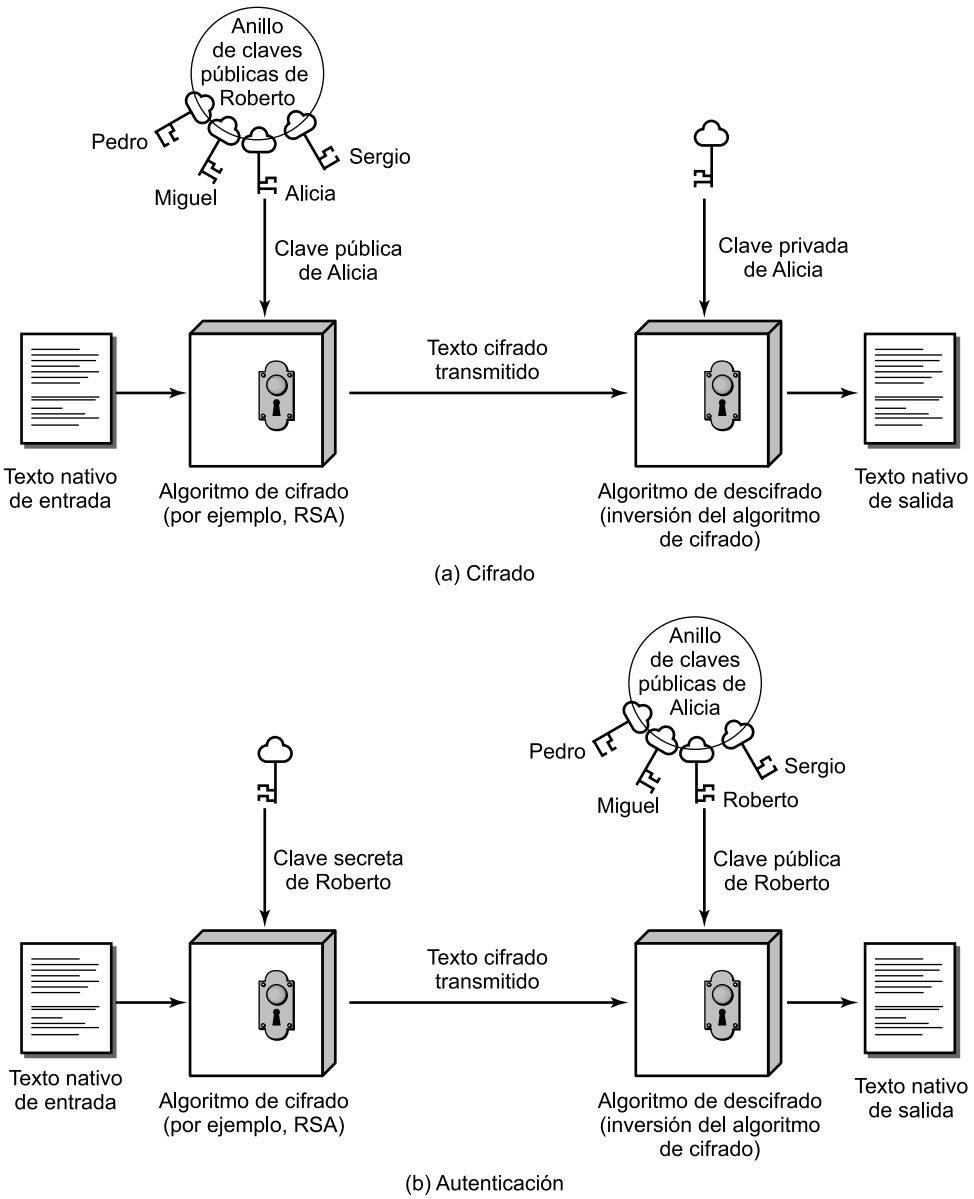


Figura 21.9. Cifrado de clave pública.

Un esquema de cifrado de clave pública se compone de seis ingredientes (*véase* Figura 21.9):

- **Texto nativo:** es el mensaje legible o los datos que se suministran como entrada al algoritmo.
- **Algoritmo de cifrado:** el algoritmo de cifrado lleva a cabo varias transformaciones sobre el texto nativo.
- **Claves pública y privada:** este es un par de claves que han sido seleccionadas para que, si una se utiliza para el cifrado, la otra se use para el descifrado. Las transformaciones concretas que realiza el algoritmo de cifrado dependen de la clave pública o privada que se suministre como entrada.

- **Texto cifrado:** es el mensaje desordenado producido como salida. Depende del texto nativo y de la clave. Para un mensaje dado, dos claves diferentes producirán dos textos cifrados diferentes.
- **Algoritmo de descifrado:** este algoritmo acepta el texto cifrado y la clave correspondiente, produciendo el texto nativo original.

Como el propio nombre sugiere, la clave pública del par se hace pública para que la utilicen otros, mientras que la clave privada es conocida solamente por el dueño. Todo algoritmo de criptografía de clave pública de propósito general se basa en una clave para el cifrado y en una clave diferente, pero relacionada, para el descifrado. Además, estos algoritmos tienen las siguientes características importantes:

- No es factible, por limitaciones computacionales, determinar la clave de descifrado si sólo se conoce el algoritmo criptográfico y la clave de cifrado.
- Para la mayoría de los esquemas de clave pública, cualquiera de las dos claves relacionadas puede utilizarse para el cifrado, utilizando la otra para el descifrado.

Los pasos esenciales son los siguientes:

1. Cada usuario genera un par de claves que van a ser utilizadas para el cifrado y el descifrado de los mensajes.
2. Cada usuario publica una de las dos claves de cifrado en un registro público o en otro fichero accesible. Ésta es la clave pública. La clave compañera se mantiene privada. Como sugiere la Figura 21.9, cada usuario mantiene una colección de claves públicas de otros usuarios.
3. Si Roberto desea enviar un mensaje privado a Alicia, él cifra el mensaje utilizando la clave pública de Alicia.
4. Cuando Alicia recibe el mensaje, lo descifra utilizando su clave privada. Ningún otro destinatario puede descifrar el mensaje, ya que solamente Alicia conoce la clave privada de Alicia.

Con esta técnica, todos los participantes tienen acceso a las claves públicas y cada participante genera localmente su clave privada, por lo que nunca se necesita distribuirlas. Mientras un usuario proteja su clave privada, las comunicaciones entrantes son seguras. En cualquier momento, un usuario puede cambiar su clave privada y publicar la clave pública compañera para reemplazar la clave pública obsoleta.

FIRMA DIGITAL

El cifrado de clave pública se puede utilizar de otra forma, como se muestra en la Figura 21.9b. Suponga que Roberto quiere enviar un mensaje a Alicia y, aunque no es importante que el mensaje se mantenga secreto, quiere que Alicia tenga la certeza de que el mensaje proviene efectivamente de él. En este caso, Roberto utiliza su propia clave privada para cifrar el mensaje. Cuando Alicia recibe el texto cifrado, comprueba que puede descifrarlo con la clave pública de Roberto, demostrando así que el mensaje ha tenido que ser cifrado por Roberto. Nadie más tiene la clave privada de Roberto y, por tanto, nadie más ha podido crear el texto cifrado que pudo ser descifrado con su clave pública. De esta forma, todo el mensaje cifrado sirve como **firma digital**. Además, es imposible alterar el mensaje sin acceder a la clave privada de Roberto, por lo que el mensaje está autenticado en términos de origen e integridad de los datos.

En el esquema anterior, se cifra el mensaje entero, lo que, aunque valida al autor y al contenido, requiere una gran cantidad de almacenamiento. Cada documento debe guardarse en texto nativo para su utilización, por motivos prácticos. Se debe guardar también una copia del texto cifrado para que se pueda verificar el origen y el contenido en caso de disputa. Una forma más eficiente de lograr el mismo resultado consiste en cifrar un pequeño bloque de bits que sea una función del documento. Este bloque, llamado código de autenticación, debe poseer la propiedad de que no sea factible modificar el documento sin cambiar el código de autenticación. Si el código de autenticación se cifra con la clave privada del emisor, éste sirve como una firma que verifica al origen, al contenido y a la secuencia. Un código seguro de dispersión como SHA-1 puede realizar esta función.

Es importante enfatizar que la firma digital no ofrece privacidad. Es decir, el mensaje que se envía está seguro frente a alteraciones, pero no lo está de ser leído por otros. Esto es obvio en el caso de una firma basada en un fragmento del mensaje, ya que el resto se transmite sin cifrar. Incluso en el caso de cifrar el mensaje completo, no hay protección de privacidad, ya que cualquier observador puede descifrar el mensaje mediante la clave pública del emisor.

EL ALGORITMO DE CIFRADO DE CLAVE PÚBLICA RSA

Uno de los primeros esquemas de clave pública fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT y publicado por primera vez en 1978 [RIVE78]. El esquema RSA ha predominado desde entonces como la única aproximación al cifrado de clave pública ampliamente aceptada e implementada. RSA es un cifrador de bloque en el que el texto nativo y el texto cifrado son enteros entre 0 y $n - 1$, para algún n.

Para algún texto nativo M y un bloque cifrado C, el cifrado y el descifrado se realiza de la siguiente forma:

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Ambos, emisor y receptor, deben conocer el valor de n y e. Sólo el receptor conoce el valor de d. Éste es un algoritmo de clave pública con una clave pública $KU = \{e, n\}$ y una clave privada $KR = \{d, n\}$. Para que este algoritmo sea un algoritmo de cifrado de clave pública satisfactorio, se deben cumplir los siguientes requisitos:

1. Es posible encontrar valores de e, d, y n tales que $M^{ed} = M \bmod n$ para todo $M < n$.
2. Es relativamente fácil calcular M^e y C^d para todos los valores de $M < n$.
3. Es impracticable determinar d dado e y n.

Los dos primeros requisitos son fáciles de satisfacer. El tercer requisito se puede satisfacer con valores altos de e y n.

La Figura 21.10 resume el algoritmo RSA. Se empieza por seleccionar dos números primos, p y q, y calcular su producto n, que es el módulo para el cifrado y el descifrado. A continuación, necesitamos la cantidad $\phi(n)$, que se conoce como totalizador de Euler de n, que es el número de enteros positivos menores que n y primos relativos de n[4]. Entonces, se selecciona un entero e que es primo relativo de $\phi(n)$ (es decir, el máximo común divisor de e y $\phi(n)$ es 1). Finalmente, se calcula d tal que $de \bmod \phi(n) = 1$. Se puede demostrar que d y e tienen las propiedades deseas.

[4] Puede demostrarse que cuando n es un producto de dos primos, pq, entonces $\phi(n) = (p - 1)(q - 1)$.

Generación de clave

Seleccionar p, q	p y q ambos primos, $p \neq q$
Calcular $n = p \times q$	
Calcular $\phi(n) = (p - 1)(q - 1)$	
Seleccionar entero e	$\text{mcd}(\phi(n), e) = 1; 1 < e < \phi(n)$
Calcular d	$de \bmod \phi(n) = 1$
Clave pública	$KU = \{e, n\}$
Clave privada	$KR = \{d, n\}$

Cifrado

Texto nativo:	$M < n$
Texto cifrado:	$C = M^e \pmod{n}$

Descifrado

Texto cifrado:	C
Texto nativo:	$M = C^d \pmod{n}$

Figura 21.10. El algoritmo RSA.

Suponga que el usuario A ha publicado su clave pública y que el usuario B quiere enviar un mensaje M a A. Para ello, B calcula $C = M^e \pmod{n}$ y transmite C. Cuando se recibe este mensaje cifrado, A lo descifra calculando $M = C^d \pmod{n}$.

En la Figura 21.11 se muestra un ejemplo extraído de [SING99]. En este ejemplo, las claves se generaron como sigue:

1. Se seleccionan dos números primos, $p = 17$ y $q = 11$.
2. Se calcula $n = pq = 17 \times 11 = 187$.
3. Se calcula $\phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.

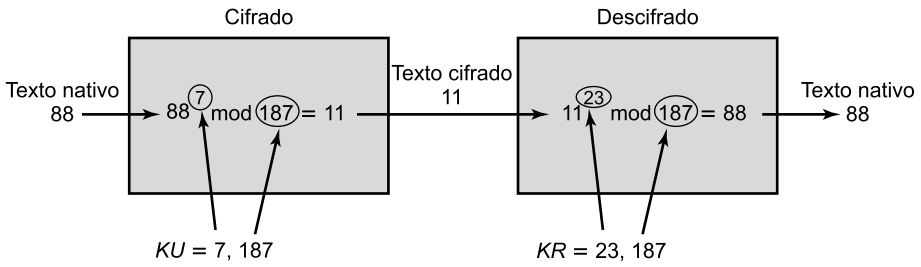


Figura 21.11. Ejemplo del algoritmo RSA.

4. Se selecciona e tal que sea primo relativo de $\phi(n) = 160$ y menor que $\phi(n)$. En este caso elegimos $e = 7$.

5. Se determina d tal que $de \bmod 160 = 1$ y $d < 160$. El valor correcto es $d = 23$, ya que $23 \times 7 = 161 = 10 \times 160 + 1$.

Las claves resultantes son la clave pública $KU = \{7, 187\}$ y la clave privada $KR = \{23, 187\}$. El ejemplo muestra el uso de estas claves para un texto nativo de entrada $M = 88$. Para el cifrado, necesitamos calcular $C = 88^7 \bmod 187$. Haciendo uso de las propiedades de la aritmética modular, podemos realizar el cálculo de la siguiente forma:

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$$88^1 \bmod 187 = 88$$

$$88^2 \bmod 187 = 7.744 \bmod 187 = 77$$

$$88^4 \bmod 187 = 59.969.536 \bmod 187 = 132$$

$$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894.432 \bmod 187 = 11$$

Para el descifrado, calculamos $M = 11^{23} \bmod 187$:

$$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$$

$$11^1 \bmod 187 = 11$$

$$11^2 \bmod 187 = 121$$

$$11^4 \bmod 187 = 14.641 \bmod 187 = 55$$

$$11^8 \bmod 187 = 214.358.881 \bmod 187 = 33$$

$$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79.720.245 \bmod 187 = 88$$

Existen dos estrategias posibles para vencer al algoritmo RSA. La primera es la estrategia de fuerza bruta: probar todas las claves privadas posibles. De este modo, cuanto mayor sea el número de bits de e y d, más seguro será el algoritmo. Sin embargo, a causa de los cálculos que requieren, tanto la generación de claves como el cifrado/descifrado son complejos y, cuanto mayor sean las longitudes de las claves, más lento funcionará el sistema.

La mayoría de las discusiones sobre el criptoanálisis de RSA se han centrado en la tarea de factorizar n en sus dos números primos. Para un n grande con factores primos altos, determinar sus factores es un problema difícil, pero no tanto como solía ser. La siguiente constituye una notable prueba de lo anterior. En 1977, los tres inventores de RSA desafiaron a los lectores de *Scientific American* a decodificar un texto cifrado que imprimieron en la columna de «Mathematical Games» de Martin Gardner. Ofrecieron 100 dólares de recompensa a quien les devolviera la frase en texto nativo, un hecho que ellos predijeron que no ocurriría en 40 cuatrillones de años. En abril de 1994, un equipo que trabajaba sobre Internet y utilizaba 1.600 computadores reclamó el premio después de sólo 8 meses de trabajo [LEUT94]. Este reto utilizaba un tamaño de clave pública (longitud de n) de 129 dígitos decimales, alrededor de 428 bits. Este resultado no invalida el uso de RSA. Simplemente significa que se deben utilizar tamaños de clave mayores. Actualmente, se considera que una clave de 1024 bits (sobre unos 300 dígitos decimales) es suficientemente robusta para, virtualmente, todo tipo de aplicaciones.

GESTIÓN DE CLAVES

En el cifrado simétrico, un requisito fundamental para que dos partes se comuniquen de una forma segura es que compartan una clave secreta. Supongamos que Roberto quiera crear una aplicación para enviar mensajes que le permita intercambiar correo electrónico de forma segura con cualquiera que tenga acceso a Internet o a alguna otra red que ambos compartan. Supongamos que Roberto quiere utilizar sólo cifrado simétrico. Con el cifrado simétrico, Roberto y su corresponsal, digamos, Alicia, deben plantearse una manera para compartir una clave secreta única que nadie más conozca. ¿Cómo van a hacer esto? Si Alicia está en la habitación contigua, Roberto puede generar la clave y escribirla en un papel o almacenarla en un disquete y entregársela a Alicia. Pero si Alicia está en la otra parte del continente o del mundo, ¿qué puede hacer Roberto? Bien, podría cifrar la clave utilizando cifrado simétrico y enviarla por correo electrónico a Alicia, pero esto significa que Roberto y Alicia deben compartir una clave secreta para poder cifrar esta nueva clave secreta. Más aún, Roberto y cualquiera que utilice este nuevo paquete de correo electrónico se debe enfrentar al mismo problema con cualquier potencial corresponsal: cada pareja de corresponsales debe compartir una clave secreta única.

El problema más difícil para utilizar cifrado simétrico consiste en cómo distribuir las claves secretas de forma segura. Este problema desaparece en el cifrado de clave pública por el simple hecho de que nunca se distribuye la clave privada. Si Roberto quiere establecer correspondencia con Alicia y otras personas, genera un único par de claves, una privada y otra pública. Entonces guarda la clave privada de forma segura y difunde la clave pública a todos sin excepción. Si Alicia hace lo mismo, entonces Roberto tiene la clave pública de Alicia, Alicia tiene la clave pública de Roberto y ya pueden comunicarse con seguridad. Cuando Roberto desee comunicarse con Alicia, puede hacer lo siguiente:

1. Preparar un mensaje.
2. Cifrar el mensaje utilizando cifrado simétrico con una clave simétrica de sesión de un solo uso.
3. Cifrar la clave de sesión utilizando cifrado de clave pública con la clave pública de Alicia.
4. Adjuntar la clave de sesión cifrada al mensaje y enviarlo a Alicia.

Solamente Alicia es capaz de descifrar la clave de sesión y, por tanto, de recuperar el mensaje original.
Para ser justos cabe señalar, sin embargo, que hemos sustituido un problema por otro. La clave privada de Alicia es segura ya que no necesita revelarla nunca. Sin embargo, Roberto ha de estar seguro de que la clave pública con el nombre de Alicia escrita en ella es de hecho la clave pública de Alicia. Alguien podría haber difundido una clave pública y haber dicho que era la de Alicia.

La solución a este problema es el **certificado de clave pública**. En esencia, un certificado consta de una clave pública más un identificador de usuario del propietario de la clave, todo ello firmado por una tercera parte de confianza. Normalmente la tercera parte es una autoridad de certificación (CA, *Certificate Authority*) en la que confía la comunidad de usuarios, como una agencia del gobierno o una institución financiera. Un usuario puede presentar su clave pública a la autoridad de un modo seguro y obtener un certificado. El usuario puede entonces publicar el certificado. Cualquiera que necesite la clave pública de este usuario puede obtener el certificado y verificar que es válido mediante la firma adjunta en que se confía. En la Figura 21.12 se muestra este proceso.

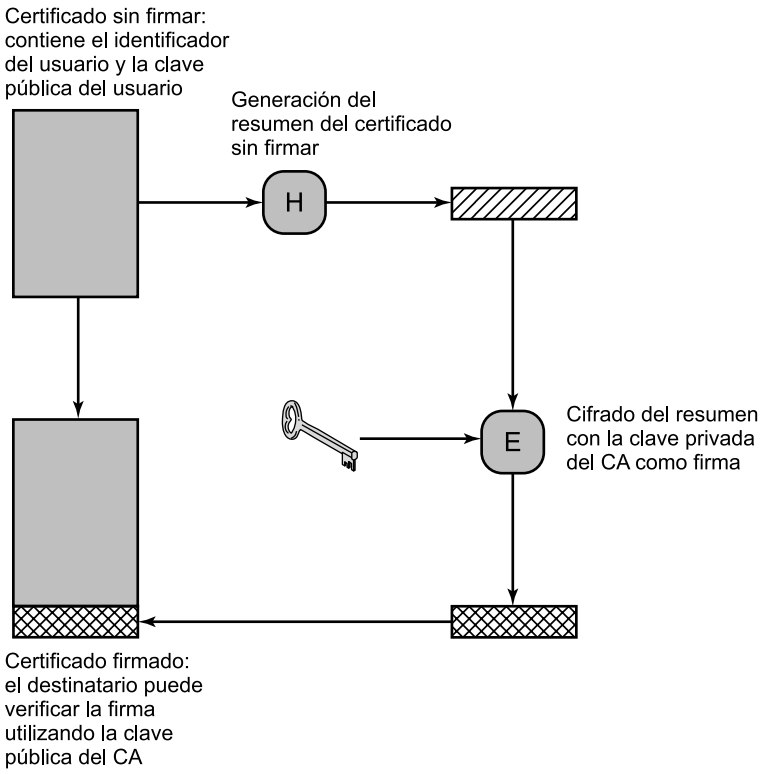


Figura 21.12. Uso del certificado de clave pública.

21.5. CAPA DE *SOCKETS* SEGURA (SSL) Y CAPA DE TRANSPORTE SEGURA (TLS)

Uno de los servicios de seguridad más ampliamente utilizados es el de capa de sockets segura (SSL) y el posterior estándar de Internet conocido como capa de transporte segura (TLS), definido este último en el RFC 2246. SSL es un servicio de propósito general implementado como un conjunto de protocolos que hacen uso de TCP. En este nivel, existen dos elecciones de implementación. Para una completa generalidad, SSL (o TLS) podría suministrarse como parte de la familia de protocolos subyacente y, de esta forma, ser transparente a las aplicaciones. Alternativamente, SSL puede integrarse en paquetes específicos. Por ejemplo, los navegadores Netscape y Microsoft Explorer vienen equipados con SSL y la mayoría de los servidores web implementan este protocolo.

Esta sección discute SSLv3. En TLS sólo existen modificaciones menores.

ARQUITECTURA SSL

SSL está diseñada para hacer uso de TCP con objeto de proporcionar un servicio fiable y seguro extremo a extremo. SSL no es un único protocolo sino dos capas de protocolos, como se ilustra en la Figura 21.13.

El protocolo de registro de SSL proporciona servicios básicos de seguridad a varios protocolos de capas superiores. En particular, el protocolo de transferencia de hipertexto (HTTP), que propor-

Protocolo de negociación bilateral de SSL
Protocolo de cambio de especificación de cifrado de SSL
Protocolo de alerta de SSL
HTTP
Protocolo de registro de SSL
TCP
IP

Figura 21.13. Pila de protocolos de SSL.

ciona el servicio de transferencia para la interacción entre cliente y servidor web, puede operar sobre SSL. Tres protocolos de capas superiores se definen como parte de SSL: el protocolo de negociación bilateral, el protocolo de cambio de especificación del cifrado, y el protocolo de alerta. Estos protocolos específicos de SSL se utilizan en la gestión de los intercambios SSL y serán examinados más adelante en esta sección.

Dos conceptos importantes de SSL son la sesión SSL y la conexión SSL, que se definen en la especificación de la siguiente forma:

- **Conexión:** una conexión es un transporte (tal y como se define en el modelo de capas OSI) que proporciona un tipo de servicio adecuado. En SSL, dichas conexiones son relaciones entre pares. Las conexiones son transitorias. Cada conexión se asocia con una sesión.
- **Sesión:** una sesión SSL es una asociación entre un cliente y un servidor. Las sesiones las crea el protocolo de negociación bilateral. Éstas definen un conjunto de parámetros de seguridad criptográficos, que pueden compartirse entre múltiples conexiones. Las sesiones se utilizan para evitar la costosa negociación de nuevos parámetros de seguridad para cada conexión.

Entre cualquier par de entidades (aplicaciones como HTTP en un cliente y un servidor), pueden existir múltiples conexiones seguras. En teoría, puede haber además múltiples sesiones simultáneas entre partes, pero esta característica no se utiliza en la práctica.

PROTOCOLO DE REGISTRO DE SSL

El protocolo de registro de SSL proporciona dos servicios para las conexiones SSL:

- **Privacidad:** el protocolo de negociación bilateral establece una clave secreta compartida que es utilizada para el cifrado simétrico de cargas útiles SSL.
- **Integridad del mensaje:** el protocolo de negociación bilateral también define una clave secreta que se utiliza para formar un código de autenticación de mensaje (MAC).

La Figura 21.14 muestra el funcionamiento general del protocolo de registro de SSL. El primer paso es la **fragmentación**. Se fragmenta cada mensaje de la capa superior en bloques de 2^{14} bytes (16.384 bytes) o menos. A continuación, opcionalmente, se aplica **compresión**. El siguiente paso en el procesamiento es calcular un **código de autenticación de mensaje** sobre los datos comprimidos. Después, el mensaje comprimido más el MAC son cifrados utilizando un cifrado simétrico.

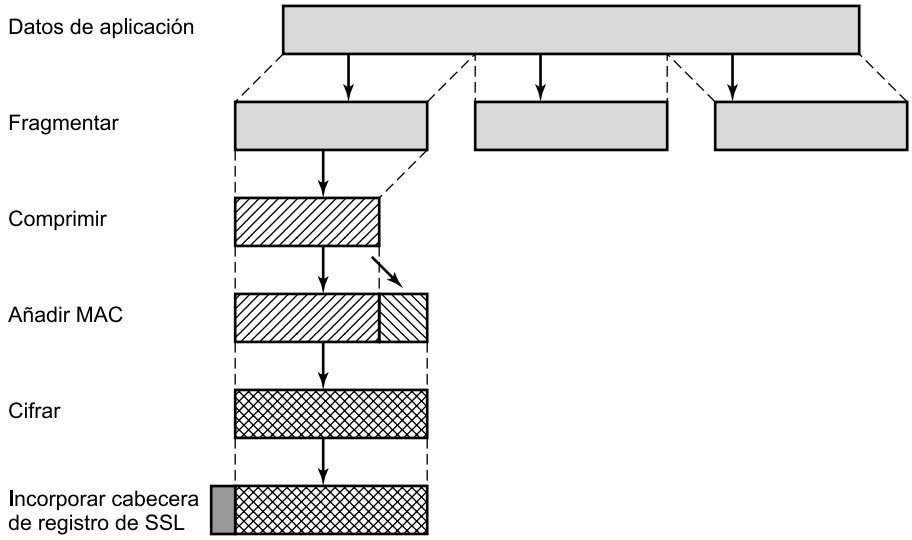


Figura 21.14. Funcionamiento del protocolo de registro de SSL.

El último paso del procesamiento del protocolo de registro de SSL consiste en insertar una cabecera que consta de los siguientes campos:

- **Tipo de contenido (8 bits):** indica el protocolo de la capa superior utilizado para procesar el fragmento adjunto.
- **Número principal de versión (8 bits):** indica el número principal de la versión de SSL que se utiliza. Para SSLv3 este valor es 3.
- **Número secundario de versión (8 bits):** indica el número secundario de la versión de SSL que se utiliza. Este valor es 0 para SSLv3.
- **Longitud de la compresión (16 bits):** se trata de la longitud en bytes del fragmento de texto nativo (o del fragmento comprimido si se ha utilizado compresión). Su valor máximo es $2^{14} + 2.048$.

Los tipos de contenido que han sido definidos son «cambio de especificación de cifrado», «alerta», «negociación bilateral», y «datos de aplicación». Los primeros tres son los protocolos específicos de SSL, discutidos a continuación. Observe que no se distingue entre las distintas aplicaciones (por ejemplo, HTTP) que podrían utilizar SSL. El contenido de los datos creados por tales aplicaciones es opaco a SSL.

El protocolo de registro transmite después la unidad resultante en un segmento TCP. Los datos recibidos se descifran, verifican, descomprimen y reensamblan y entonces se entregan a los usuarios de niveles superiores.

PROTOCOLO DE CAMBIO DE ESPECIFICACIÓN DE CIFRADO

El protocolo de cambio de especificación de cifrado es uno de los tres protocolos específicos de SSL que usa el protocolo de registro de SSL, siendo el más simple. Este protocolo consta de un solo mensaje, que consiste en un solo byte con el valor 1. El único propósito de este mensaje es provocar que se copie el estado pendiente en el estado actual, lo que actualiza el repertorio de cifrado a utilizar en esta conexión.

PROTOCOLO DE ALERTA

El protocolo de alerta se usa para transportar las alertas relacionadas con SSL a la entidad par. Como con otras aplicaciones que usan SSL, los mensajes de alerta se comprimen y cifran, según lo especificado en el estado actual.

Cada mensaje de este protocolo consta de dos bytes. El primer byte toma el valor «advertencia» (1) o «fatal» (2) para transmitir la gravedad del mensaje. Si el nivel es fatal, SSL termina inmediatamente la conexión. Otras conexiones de la misma sesión pueden continuar, pero no se pueden establecer nuevas conexiones en esta sesión. El segundo byte contiene un código que describe la alerta concreta. Un ejemplo de una alerta fatal es el de un MAC incorrecto. Un ejemplo de una alerta no fatal es el de un mensaje notificar cierre, que notifica al destinatario que el emisor no enviará más mensajes sobre esta conexión.

PROTOCOLO DE NEGOCIACIÓN BILATERAL

La parte más compleja de SSL es el protocolo de negociación bilateral. Este protocolo permite al servidor y al cliente autenticarse mutuamente para negociar unos algoritmos de cifrado y de MAC y las claves criptográficas que se usarán para proteger los datos enviados en los registros SSL. El protocolo de negociación bilateral se utiliza antes de que se transmita ningún dato de aplicación.

El protocolo de negociación bilateral consta de una serie de mensajes que se intercambian el cliente y el servidor. La Figura 21.15 muestra el intercambio inicial necesitado para establecer una conexión lógica entre cliente y servidor. Se pueden distinguir cuatro fases en el intercambio.

La **fase 1** se utiliza para iniciar una conexión lógica y establecer las capacidades de seguridad que se le asociarán. El intercambio lo inicia el cliente, el cual envía un mensaje «saludo de cliente» con los siguientes parámetros:

- **Versión:** la versión más alta que el cliente comprende.
- **Aleatorio:** una estructura aleatoria generada por el cliente que consta de una marca de tiempo de 32 bits y 28 bytes generados mediante un generador de números aleatorios seguro. Estos valores se utilizan durante el intercambio de clave para impedir ataques por retransmisión.
- **Identificador de la sesión:** un identificador de sesión de longitud variable. Un valor distinto de cero indica que el cliente desea actualizar los parámetros de una conexión existente o crear una nueva conexión en esta sesión. Un valor de cero indica que el cliente desea establecer una nueva conexión en una nueva sesión.
- **Repertorio de cifrado:** es una lista que contiene las combinaciones de los algoritmos criptográficos admitidos por el cliente, en orden decreciente de preferencia. Cada elemento de la lista (cada repertorio de cifrado) define tanto un algoritmo de intercambio de clave como una especificación de cifrado.
- **Método de compresión:** es una lista de los métodos de compresión que admite el cliente.

Tras enviar el mensaje «saludo de cliente», el cliente espera el mensaje «saludo de servidor», el cual contiene los mismos parámetros que el mensaje de «saludo de cliente».

Los detalles de la **fase 2** dependen del esquema de cifrado de clave pública subyacente utilizado. En algunos casos, el servidor pasa un certificado al cliente, posible información adicional de la clave y una solicitud del certificado del cliente.

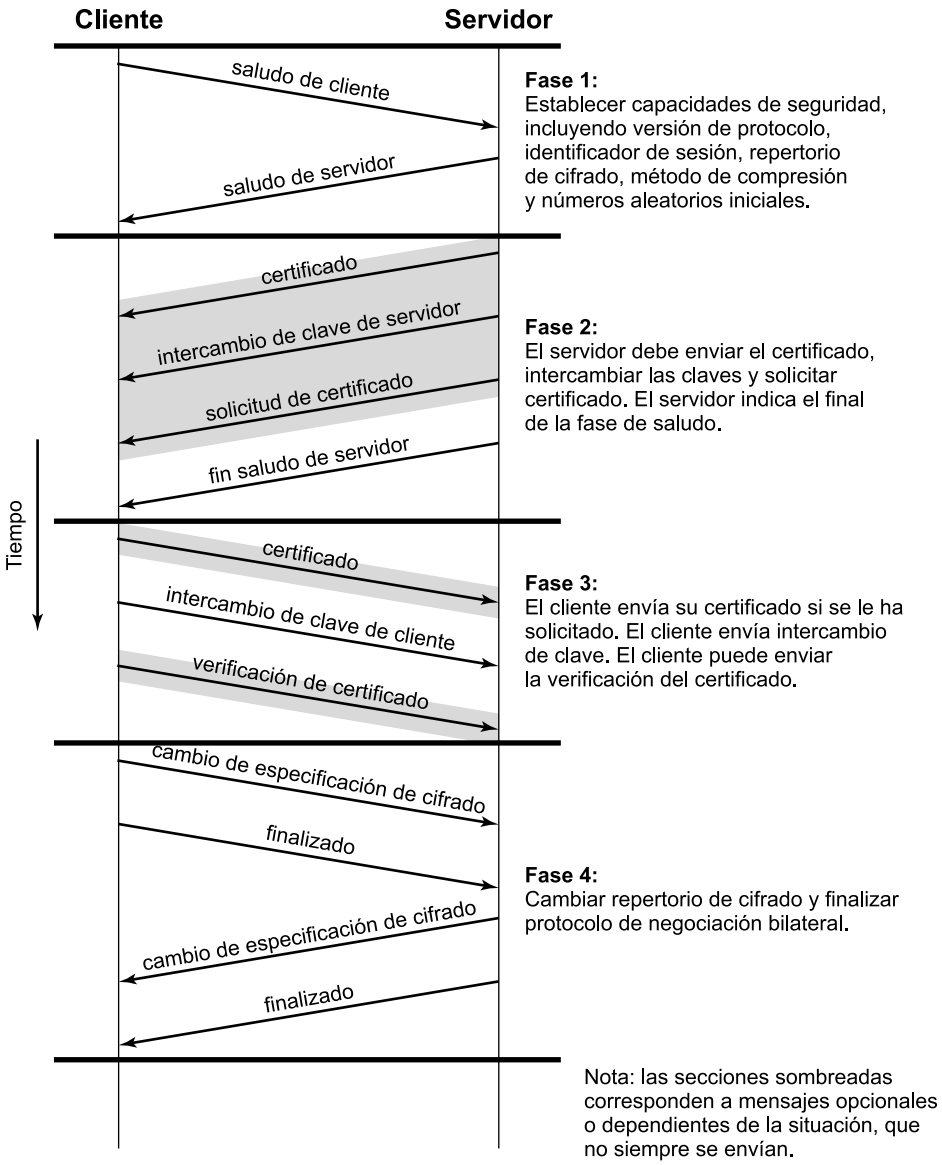

Cliente
Servidor
saludo de cliente
saludo de servidor
Fase 1:
Establecer capacidades de seguridad, incluyendo versión de protocolo, identificador de sesión, repertorio de cifrado, método de compresión y números aleatorios iniciales.
certificado
intercambio de clave de servidor
solicitud de certificado
fin saludo de servidor
Fase 2:
El servidor debe enviar el certificado, intercambiar las claves y solicitar certificado. El servidor indica el final de la fase de saludo.
Tiempo
certificado
intercambio de clave de cliente
verificación de certificado
Fase 3:
El cliente envía su certificado si se le ha solicitado. El cliente envía intercambio de clave. El cliente puede enviar la verificación del certificado.
cambio de especificación de cifrado
finalizado
cambio de especificación de cifrado
finalizado
Fase 4:
Cambiar repertorio de cifrado y finalizar protocolo de negociación bilateral.
Nota: las secciones sombreadas corresponden a mensajes opcionales o dependientes de la situación, que no siempre se envían.

Figura 21.15. Funcionamiento del protocolo de negociación bilateral.

El mensaje final en la fase 2, siempre requerido, es el mensaje «fin saludo de servidor», que envía el servidor para indicar el fin de los mensajes de saludo y asociados. Tras enviar este mensaje, el servidor esperará una respuesta del cliente.

En la **fase 3**, al recibir el mensaje «fin saludo de servidor», el cliente debe verificar que el servidor proporcionó un certificado válido, si es necesario, y verificar que los parámetros del mensaje «saludo de servidor» se aceptan. Si todo es satisfactorio, el cliente envía uno o más mensajes de vuelta al servidor, dependiendo del esquema de clave pública subyacente.

La **fase 4** completa el establecimiento de una conexión segura. El cliente envía un mensaje «cambio de especificación de cifrado» y copia la especificación de cifrado pendiente sobre la espe-

cificación de cifrado actual. Observe que este mensaje no se considera parte del protocolo de negociación bilateral, sino que se envía utilizando el protocolo de especificación de cambio de cifrado. El cliente envía inmediatamente el mensaje «finalizado» bajo los nuevos algoritmos, claves y secretos. El mensaje «finalizado» verifica que los procesos de intercambio de clave y autenticación fueron satisfactorios.

En respuesta a esos dos mensajes, el servidor envía su propio mensaje de «cambio de especificación de cifrado», transfiere la especificación de cifrado pendiente a la actual y envía su mensaje «finalizado». En este punto, la negociación bilateral está completa y el cliente y el servidor pueden empezar a intercambiar datos de la capa de aplicación.

21.6. SEGURIDAD EN IPV4 E IPV6

En 1994, la Junta de Arquitectura de Internet (IAB, *Internet Architecture Board*) publicó un informe titulado «Seguridad en la arquitectura de Internet» (RFC 1636). El informe exponía el consenso general de que Internet necesita más y mejor seguridad e identificaba las áreas clave para mecanismos de seguridad. Entre estos se encontraban la necesidad de asegurar la infraestructura de red contra la monitorización no autorizada, el control del tráfico de red y la necesidad de asegurar el tráfico de usuario final a usuario final utilizando mecanismos de autenticación y cifrado.

Estas preocupaciones están plenamente justificadas. Como confirmación, el informe anual de 2002 del Equipo de Respuesta a Emergencias en Computadores (CERT, *Computer Emergency Response Team*) enumeraba alrededor de 82.000 informes sobre incidentes de seguridad [CERT03]. Los tipos de ataques más serios incluían la falsificación de dirección IP (*IP spoofing*), en la que un intruso crea paquetes con direcciones IP falsas y explota las aplicaciones que utilizan la autenticación basada en direcciones IP. También se incluían varias formas de escuchas y captura de paquetes (*packet sniffing*), en las que los atacantes leen la información transmitida, incluyendo información de ingreso en sistemas y contenido de bases de datos.

En respuesta a estas cuestiones, el IAB incluyó la autenticación y el cifrado como características de seguridad necesarias en el protocolo IP de nueva generación, que ha sido emitido como IPv6. Afortunadamente, estas capacidades de seguridad se diseñaron para que fueran utilizables tanto en IPv4 como en IPv6. Esto significa que los fabricantes ya pueden empezar a ofrecer estas características y muchos de ellos incluyen actualmente algunas capacidades de IPSec en sus productos.

APLICACIONES DE IPSec

IPSec proporciona la capacidad de asegurar las comunicaciones que se efectúen a través de una LAN, a través de una WAN privada o pública y a través de Internet. Algunos ejemplos de su uso incluyen los siguientes:

- **Conectividad segura entre sucursales a través de Internet:** una compañía puede construir una red privada virtual sobre Internet o a través de una WAN pública. Esto permite a un negocio apoyarse firmemente en Internet y reducir su necesidad de una red privada, ahorrando costes y gestión de red adicional.
- **Acceso remoto seguro a través de Internet:** un usuario final cuyo sistema esté equipado con protocolos de seguridad de IP puede realizar una llamada local a un proveedor de servicios de Internet (ISP, *Internet Service Provider*) y obtener un acceso seguro a la red de una

compañía. Esto reduce el coste de los gastos de los empleados itinerantes y de los trabajadores a distancia.

- **Establecimiento de conectividad intranet y extranet con socios:** IPSec se puede utilizar para asegurar la comunicación con otras organizaciones, asegurando la autenticación y la privacidad y proporcionando un mecanismo de intercambio de claves.
- **Mejora de la seguridad en el comercio electrónico:** aunque algunas aplicaciones web y de comercio electrónico tienen protocolos de seguridad integrados, la utilización de IPSec mejora esa seguridad.

La principal característica de IPSec que le permite dar soporte a estas diversas aplicaciones consiste en que puede cifrar y/o autenticar *todo* el tráfico a nivel IP. Así, todas las aplicaciones distribuidas, incluyendo la conexión remota, las aplicaciones cliente/servidor, el correo electrónico, la transferencia de ficheros, el acceso a la web, etc., pueden hacerse seguras.

ÁMBITO DE IPSec

IPSec proporciona tres servicios principales: una función de sólo autenticación conocida como cabecera de autenticación (AH, *Authentication Header*), una función combinada de autenticación/cifrado llamada encapsulado de la carga útil de seguridad (ESP, *Encapsulating Security Payload*), y una función de intercambio de claves. Para redes privadas virtuales se desea generalmente autenticación y cifrado, ya que es importante tanto (1) asegurar que usuarios no autorizados no entran en la red privada virtual como (2) asegurar que si hay observadores en Internet no puedan leer los mensajes enviados por la red privada virtual. Dado que ambas características son deseables, la mayoría de las implementaciones utilizan ESP en lugar de AH. La función de intercambio de claves permite el intercambio manual de claves así como un esquema automático.

La especificación de IPSec es bastante compleja y comprende numerosos documentos. Los más importantes, publicados en noviembre de 1998, son los RFC 2401, 2402, 2406 y 2408. En esta sección se proporciona una visión general de algunos de los elementos más importantes de IPSec.

ASOCIACIONES DE SEGURIDAD

Un concepto clave que aparece tanto en los mecanismos de autenticación como de privacidad en IP es la asociación de seguridad (SA, *Security Association*). Una asociación es una relación en un solo sentido entre un emisor y un receptor que proporciona servicios de seguridad al tráfico que transporta. Si se necesita una relación paritaria, para un intercambio seguro en dos sentidos, entonces se requieren dos asociaciones de seguridad. Los servicios de seguridad se proporcionan a una SA para que utilice AH o ESP, pero no ambos.

Una asociación de seguridad está identificada unívocamente por tres parámetros:

- **Índice de parámetros de seguridad (SPI, *Security Parameters Index*):** una cadena de bits asignada a esta SA y con significado local solamente. El SPI se transporta en las cabeceras AH y ESP para permitir que el sistema receptor seleccione la SA bajo la que se procesará un paquete recibido.
- **Dirección IP destino:** actualmente sólo se permiten direcciones de unidifusión. Ésta es la dirección del extremo destino de la SA, que puede ser un usuario final o un sistema de red, como un cortafuegos o un dispositivo de encaminamiento.

- **Identificador del protocolo de seguridad:** distingue entre una asociación de seguridad de AH o de ESP.

Por tanto, en cualquier paquete IP, la asociación de seguridad está unívocamente identificada por la dirección destino de la cabecera IPv4 o IPv6 y el SPI incluido en la cabecera de extensión (AH o ESP).

Una implementación de IPSec incluye una base de datos de asociaciones de seguridad que define los parámetros asociados con cada SA. Una asociación de seguridad se define por los parámetros siguientes:

- **Contador del número de secuencia:** un valor de 32 bits utilizado para generar el campo de número de secuencia de las cabeceras AH o ESP.
- **Desbordamiento del contador de secuencia:** un indicador que avisa de si se debe generar un evento registrable en caso de producirse un desbordamiento del contador de números de secuencia e impedir que siga la transmisión de paquetes en esta SA.
- **Ventana contra retransmisiones:** utilizada para determinar si un paquete AH o ESP recibido constituye una retransmisión, mediante la definición de una ventana deslizante dentro de la cual se ha de encontrar el número de secuencia.
- **Información de AH:** algoritmo de autenticación, claves, tiempos de validez de las claves y parámetros relacionados que se utilizan con AH.
- **Información de ESP:** algoritmos de cifrado y autenticación, claves, valores de inicialización, tiempos de validez de las claves y parámetros relacionados que se utilizan con ESP.
- **Tiempo de validez de la asociación de seguridad:** un intervalo de tiempo o contador de bytes tras los cuales una SA se ha de terminar o reemplazar por una SA nueva (y un nuevo SPI), más una indicación de cuál de estas opciones debe llevarse a cabo.
- **Modo del protocolo IPSec:** túnel, transporte o comodín (necesario en todas las implementaciones).
- **MTU de la ruta:** cualquier unidad de transferencia máxima de la ruta observada (tamaño máximo de un paquete que se puede transmitir sin fragmentación) y variables de caducidad (necesario en todas las implementaciones).

El mecanismo de gestión de claves que se utiliza para distribuir las claves está acoplado a los mecanismos de autenticación y privacidad sólo a través del índice de parámetros de seguridad. Por tanto, la autenticación y la privacidad han sido especificadas de forma independiente respecto a cualquier mecanismo específico de gestión de claves.

CABECERA DE AUTENTICACIÓN

La cabecera de autenticación proporciona soporte para la integridad de los datos y la autenticación de los paquetes IP. La característica de integridad de los datos asegura que sea posible detectar cualquier modificación del contenido de un paquete durante su tránsito. La característica de autenticación posibilita a un sistema final o a un dispositivo de red autenticar al usuario o la aplicación y filtrar el tráfico en consecuencia. También impide el ataque por falsificación de dirección observado en la actual Internet. La AH también protege frente al ataque de retransmisión descrito más adelante en esta sección.

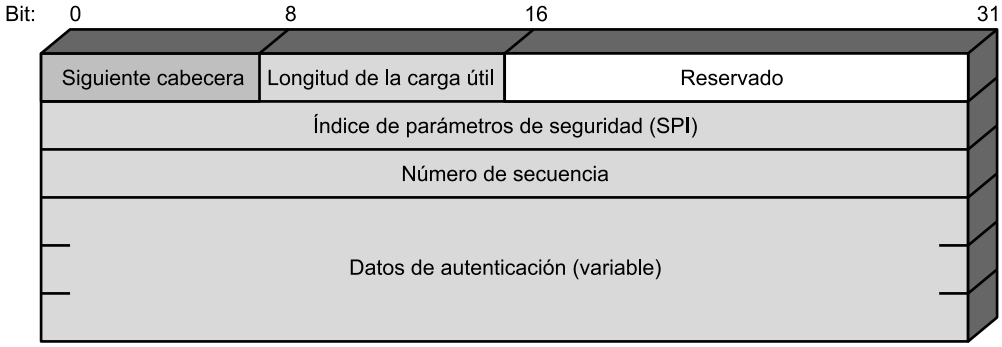


Figura 21.16. Cabecera de autenticación de IPSec.

La autenticación se basa en el uso de un código de autenticación de mensaje (MAC), tal y como se describe en la Sección 21.3. Por tanto, las dos partes deben compartir una clave secreta.

La cabecera de autenticación consta de los siguientes campos (*véase* Figura 21.16):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que aparece a continuación de ésta.
- **Longitud de la carga útil (8 bits):** longitud de la cabecera de autenticación en palabras de 32 bits, menos 2. Por ejemplo, la longitud por defecto del campo de datos de autenticación es de 96 bits, o tres palabras de 32 bits. Con una cabecera fija de tres palabras, hay un total de seis palabras en la cabecera, por lo que el campo de longitud de la carga útil vale 4.
- **Reservado (16 bits):** para uso futuro.
- **Índice de parámetros de seguridad (32 bits):** identifica una asociación de seguridad.
- **Número de secuencia (32 bits):** el valor de un contador que se incrementa de forma monótona.
- **Datos de autenticación (variable):** un campo de longitud variable (debe ser un número entero de palabras de 32 bits) que contiene el valor de comprobación de integridad (ICV, *Integrity Check Value*) o el MAC para este paquete.

El contenido del campo de datos de autenticación se calcula sobre lo siguiente:

- Los campos de la cabecera IP que no cambien en el camino (inmutables) o que tienen un valor predecible de AH SA cuando llegue al extremo. Los campos que pueden cambiar en el tránsito o que no se puedan predecir en la llegada se establecen a cero para propósitos de cálculo tanto en el origen como en el destino.
- La cabecera AH que no sea el campo de datos de autenticación. El campo de datos de autenticación se establece a cero para propósitos de cálculo tanto en el origen como en el destino.
- Todos los datos del protocolo de la capa superior, que se supone que son inmutables durante el camino.

Para IPv4, algunos ejemplos de campos inmutables son la longitud de la cabecera Internet y la dirección origen. Como ejemplo de campo sujeto a cambios pero predecible es la dirección destino (en el encaminamiento por la fuente estricto o aproximado). Ejemplos de campos sujetos a cambios que se establecen a cero antes de los cálculos del ICV son los campos de tiempo de vida y

suma de comprobación. Observe que los campos de dirección origen y destino están protegidos, impidiéndose así la falsificación de la dirección.

Para IPv6, algunos ejemplos en la cabecera base son la versión (inmutable), la dirección destino (sujeto a cambios pero predecible) y la etiqueta de flujo (sujeto a cambios y puesto a cero para los cálculos).

ENCAPSULADO DE LA CARGA ÚTIL DE SEGURIDAD

El encapsulado de la carga útil de seguridad proporciona servicios de privacidad, incluyendo privacidad del contenido de los mensajes y una limitada privacidad del flujo de tráfico. Como una característica opcional, ESP puede también proporcionar un servicio de autenticación.

La Figura 21.17 muestra el formato de un paquete ESP. Contiene los siguientes campos:

- **Índice de parámetros de seguridad (32 bits):** identifica una asociación de seguridad.
- **Número de secuencia (32 bits):** el valor de un contador que se incrementa de forma monótona.
- **Datos de la carga útil (variable):** se trata de un segmento de la capa superior protegido mediante cifrado.
- **Relleno (0-255 octetos):** este campo puede requerirse si el algoritmo de cifrado necesita que el texto nativo sea un múltiplo de algún número de bytes.
- **Longitud del relleno (8 bits):** indica el número de bytes de relleno que preceden inmediatamente a este campo.
- **Cabecera siguiente (8 bits):** identifica el tipo de datos contenidos en el campo de datos de carga útil mediante la identificación de la primera cabecera en esa carga útil (por ejemplo, una cabecera de extensión de IPv6 o un protocolo de una capa superior como TCP).

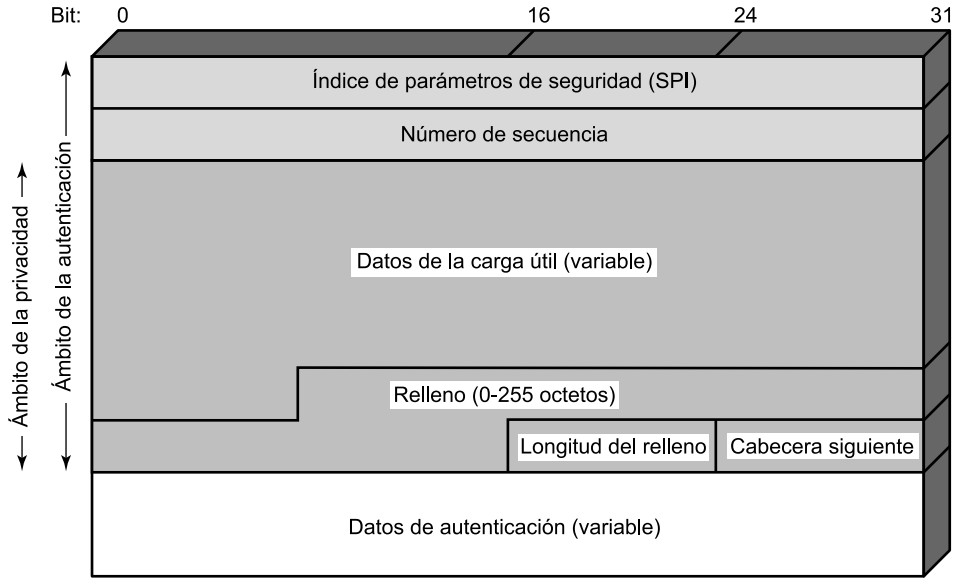


Figura 21.17. Formato del ESP de IPSec.

- **Datos de autenticación (variable):** Un campo de longitud variable (debe ser un número entero de palabras de 32 bits) que contiene el valor de comprobación de integridad calculado sobre el paquete ESP menos el campo de datos de autenticación.

21.7. LECTURAS Y SITIOS WEB RECOMENDADOS

Los temas de este capítulo se tratan con un mayor detalle en [STAL03]. Para más información sobre los algoritmos de criptografía, [SCHN96] constituye un trabajo de referencia esencial. Contiene descripciones, virtualmente, de cada algoritmo y protocolo criptográfico publicado en los últimos 15 años.

SCHN96 Schneier, B. *Applied Cryptography*. New York: Wiley, 1996.

STAL03 Stallings, W. *Cryptography and Network Security: Principles and Practice, 3rd ed.,* Upper Saddle River, NJ: Prentice Hall, 2003.

SITIOS WEB RECOMENDADOS

- **COAST:** se trata de un completo conjunto de enlaces relacionados con la criptografía y la seguridad de red.
- **Área de seguridad de la IEFT:** proporciona información actualizada de las propuestas de estandarización sobre seguridad en Internet.
- **Comité Técnico de IEEE sobre seguridad y privacidad:** proporciona copias de los boletines de IEEE e información sobre actividades relacionadas de IEEE.

21.8. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y EJERCICIOS

TÉRMINOS CLAVE

algoritmo de cifrado
algoritmo de descifrado
análisis de tráfico
ataque activo
ataque pasivo
ataque por fuerza bruta
autenticación de mensajes
autenticidad
capa de *sockets* segura (SSL)
capa de transporte segura (TLS)
centro de distribución de claves (KDC)
certificado de clave pública
cifrado de clave pública
cifrado simétrico
clave de sesión
clave privada
clave pública
clave secreta
código de autenticación de mensajes (MAC)
criptoanálisis
denegación de servicio
disponibilidad
distribución de clave
enmascaramiento
estándar de cifrado avanzado (AES)
estándar de cifrado de datos (DES)
firma digital
función de dispersión
función de dispersión de un solo sentido
función de dispersión segura

gestión de claves
integridad
privacidad
relleno de tráfico
retransmisión
RSA
seguridad IP (IPSec)
SHA-1
texto cifrado
texto nativo

CUESTIONES DE REPASO

21.1. ¿Cuál es la diferencia existente entre amenazas de seguridad pasivas y activas?

21.2. Enumere y defina brevemente categorías de amenazas de seguridad pasivas y activas.

21.3. ¿Qué son DES y triple DES?

21.4. ¿Cómo se espera que AES suponga una mejora con respecto a triple DES?

21.5. Explique en qué consiste el relleno de tráfico.

21.6. Enumere y defina brevemente varias alternativas para la autenticación de mensajes.

21.7. ¿Qué es una función de dispersión segura?

21.8. Explique la diferencia existente entre el cifrado simétrico y el cifrado de clave pública.

21.9. ¿Cuáles son las diferencias entre los términos *clave pública*, *clave privada* y *clave secreta*?

21.10. ¿Qué es una firma digital?

21.11. ¿Qué es un certificado de clave pública?

21.12. ¿Qué protocolos comprende SSL?

21.13. ¿Cuál es la diferencia entre una conexión SSL y una sesión SSL?

21.14. ¿Qué servicios proporciona el protocolo de registro de SSL?

21.15. ¿Qué servicios proporciona IPSec?

EJERCICIOS

21.1. Dé algunos ejemplos donde el análisis del tráfico pueda comprometer la seguridad. Describa situaciones donde el cifrado extremo a extremo combinado con el cifrado de enlace permitiría todavía suficiente análisis de tráfico como para que fuera peligroso.

21.2. Los esquemas de distribución de claves que utilizan un centro de control de accesos y/o un centro de distribución de claves tienen puntos centrales vulnerables a ataques. Discuta las implicaciones en la seguridad de tal centralización.

21.3. Suponga que alguien sugiere la siguiente forma para confirmar que dos de ustedes están en posesión de la misma clave secreta. Usted crea una cadena de bits aleatoria con longitud igual a la de la clave, realiza la operación XOR entre la cadena y la clave y envía el resultado por el canal. Su pareja realiza la operación XOR del bloque recibido con la clave (que debería ser la misma) y envía el resultado de vuelta. Usted la comprueba y, si recibe la cadena de bits original, se ha verificado que su pareja tiene la misma clave sin tener que transmitirla ni usted ni el otro participante en ningún momento. ¿Hay algún defecto en este esquema?

21.4. Antes del descubrimiento de cualquier esquema específico de clave pública, como es RSA, se desarrolló una demostración de su existencia, cuyo propósito fue demostrar que el cifrado de clave pública era posible en teoría. Considere las funciones $f_1(x_1) = z_1$, $f_2(x_2, y_2) = z_2$, $f_3(x_3, y_3) = z_3$, donde todos los valores son enteros con $1 \leqslant x_i$, y_i, $z_i \leqslant N$. La función f_1 se puede representar por un vector M1 de longitud N, en el que la entrada k-ésima es el valor de $f_1(k)$. De igual forma, f_2 y f_3 se pueden representar por las matrices M2 y M3 de dimensión $N \times N$. Se pretende representar el proceso de cifrado/descifrado mediante búsquedas en tablas con valores de N muy altos. Tales tablas serían en la práctica demasiado grandes, pero en principio podrían construirse. El esquema funciona de la siguiente manera: construya M1 con una permutación aleatoria de todos lo enteros entre 1 y N. Es decir, que cada entero aparezca una sola vez exactamente. Construya M2 de forma que cada fila contenga una permutación aleatoria de los N primeros enteros. Finalmente, rellene M3 para que satisfaga la siguiente condición:

$$f_3(f_2(f_1(k), p), k) = p \text{ para todo } k, p \text{ con } 1 \leqslant k, p \leqslant N$$

En otras palabras:

1. M1 toma como entrada k y produce una salida x.

2. M2 toma como entrada x y p, dando z como salida.

3. M3 toma como entrada z y k, y produce p.

Las tres tablas, una vez construidas, se hacen públicas.

a) Debe quedar claro que es posible construir M3 de forma que satisfaga la condición anterior. Como ejemplo, rellene M3 para el caso simple siguiente:

M1 =

5
4
2
3
1

M2 =

5	2	3	4	1
4	2	5	1	3
1	3	2	4	5
3	1	4	2	5
2	5	3	4	1

M3 =

Convención: el elemento i-ésimo de M1 corresponde a $k = i$. La fila i-ésima de M2 corresponde a $x = i$. La columna j-ésima de M2 corresponde a $p = j$. La fila i-ésima de M3 corresponde a $z = i$. La columna j-ésima de M3 corresponde a $k = j$.

b) Describa la utilización de este conjunto de tablas para llevar a cabo el cifrado y el descifrado entre dos usuarios.

c) Razone que éste es un esquema seguro.

21.5. Lleve a cabo el cifrado y el descifrado utilizando el algoritmo RSA, como en la Figura 21.11, con los siguientes valores:

a) $p = 3$; $q = 11$, $d = 7$; $M = 5$

b) $p = 5$; $q = 11$, $e = 3$; $M = 9$

c) $p = 7; \quad q = 11, \quad e = 17; \quad M = 8$

d) $p = 11; \quad q = 13, \quad e = 11; \quad M = 7$

e) $p = 17; \quad q = 31, \quad e = 7; \quad M = 2.$

Sugerencia: el descifrado no es tan difícil como se piensa. Utilice alguna sutileza.

21.6. En un sistema de clave pública que utiliza RSA se intercepta el texto cifrado $C = 10$ enviado a un usuario cuya clave pública es $e = 5$, $n = 35$. ¿Cuál es el texto nativo M?

21.7. En un sistema RSA, la clave pública de un usuario dado es $e = 31$, $n = 3.599$. ¿Cuál es la clave privada de este usuario?

21.8. Suponga que se tiene un conjunto de bloques codificado con el algoritmo RSA y que no se tiene la clave privada. Suponga que $n = pq$, e es la clave pública. Suponga además que alguien comenta que conoce que uno de los bloques de texto nativo tiene un factor común con n. ¿Puede esto ayudar de alguna forma?

21.9. Muestre cómo RSA puede representarse por las matrices M1, M2 y M3 del Ejercicio 21.4.

21.10. Considere el siguiente esquema:

1. Elija un número impar, E.

2. Elija dos números primos, P y Q, donde $(P - 1)(Q - 1) - 1$ es divisible por E.

3. Multiplique P y Q para obtener N.

4. Calcule $D = \dfrac{(P - 1)(Q - 1)(E - 1) + 1}{E}$

¿Es equivalente este esquema a RSA? Demuestre su respuesta.

21.11. Considere la utilización de RSA con una clave conocida para construir una función de dispersión de un solo sentido. Después, procese de la siguiente manera un mensaje constituido por una secuencia de bloques: cifre el primer bloque, realice la operación XOR entre el resultado y el segundo bloque y cífrelo de nuevo, y así sucesivamente. Demuestre que este esquema no es seguro mediante la resolución del siguiente problema: dado un mensaje de dos bloques, B1 y B2, y su función de dispersión:

$$\text{RSAH(B1, B2)} = \text{RSA(RSA(B1)} \oplus \text{B2)}$$

y dado un bloque arbitrario C1, elegir C2 para que RSAH(C1, C2) = RSAH(B1, B2).

21.12. En SSL y TLS, ¿por qué existe un protocolo de cambio de especificación de cifrado separado en vez de incluir un mensaje de «cambio de especificación de cifrado» en el protocolo de negociación bilateral?

21.13. Cuando se discutió el procesamiento de AH se mencionó que no todos los campos de la cabecera IP se incluyen en el cálculo del MAC.

a) Para cada uno de los campos de la cabecera IPv4, indique si el campo es invariable, sujeto a modificación pero predecible o modificable (puesto a cero antes de calcular el ICV).

b) Haga lo mismo para la cabecera IPv6.

c) Haga lo mismo para las cabeceras de extensión IPv6.

En cada caso, justifique su decisión para cada campo.

CAPÍTULO 22

Aplicaciones distribuidas

22.1. Correo electrónico—SMTP y MIME
Protocolo simple de transferencia de correo (SMTP)
Extensiones multipropósito de correo electrónico (MIME)

22.2. Protocolo de transferencia de hipertexto (HTTP)
Descripción general de HTTP
Mensajes
Mensajes de solicitud
Mensajes de respuesta
Entidades

22.3. Gestión de red—SNMP
Sistemas de gestión de red
Protocolo simple de gestión de red, versión 1 (SNMPv1)
Protocolo simple de gestión de red, versión 2 (SNMPv2)
Protocolo simple de gestión de red, versión 3 (SNMPv3)

22.4. Lecturas y sitios web recomendados

22.5. Términos clave, cuestiones de repaso y ejercicios
Términos clave
Cuestiones de repaso
Ejercicios

CUESTIONES BÁSICAS

- El protocolo más extendido para la transmisión de correo electrónico es SMTP. SMTP supone que el contenido del mensaje es un bloque de texto simple. El reciente estándar MIME amplía SMTP para permitir la transmisión de información multimedia.
- El rápido crecimiento en la utilización de la web se debe a la estandarización de todos los elementos necesarios para las aplicaciones web. Un elemento clave es HTTP, que es el protocolo para el intercambio de información basada en web entre los navegadores y los servidores web.
- El esquema estandarizado más importante para dar sustento a aplicaciones de gestión de red es el protocolo simple de gestión de red (SNMP). La versión original de SNMP está disponible en una amplia serie de productos y su utilización está muy extendida. SNMPv2 comprende diversas mejoras funcionales sobre SNMP, por lo que está reemplazándolo. SNMPv3 proporciona características de seguridad añadidas a SNMPv2.

Todos los protocolos y funciones descritos hasta ahora en la Parte V están orientados hacia un objetivo: dar soporte a las aplicaciones distribuidas que supongan la interacción de múltiples sistemas independientes. En el modelo OSI, estas aplicaciones ocupan la capa de aplicación y reciben directamente el soporte de la capa de presentación. En el conjunto de protocolos TCP/IP, dichas aplicaciones se apoyan en TCP o UDP.

En este capítulo examinaremos tres aplicaciones que familiarizarán al lector con la extensión y diversidad de las aplicaciones soportadas por una arquitectura de comunicaciones. El capítulo comienza con el correo electrónico, con los estándares SMTP y MIME como ejemplos. SMTP proporciona un servicio de correo básico, mientras que MIME añade a SMTP la posibilidad de incorporar contenido multimedia. A continuación, examinaremos HTTP, que es el protocolo sobre el que opera la telaraña mundial (WWW, *World Wide Web*). Finalmente, trataremos la gestión de la red, una aplicación de soporte diseñada para asegurar la monitorización efectiva y el control de un sistema distribuido. El protocolo concreto que examinaremos es el protocolo simple de gestión de red (SNMP), diseñado para operar tanto en los entornos TCP/IP como OSI.

En la Figura 2.15 se muestra la posición de los protocolos mostrados en este capítulo dentro de la familia de protocolos TCP/IP.

22.1. CORREO ELECTRÓNICO—SMTP Y MIME

La aplicación más utilizada virtualmente en cualquier sistema distribuido es el correo electrónico. El protocolo simple de transferencia de correo (SMTP, *Simple Mail Transfer Protocol*) ha sido siempre el caballo de batalla del conjunto de protocolos TCP/IP. Sin embargo, SMTP ha estado tradicionalmente limitado a la distribución de mensajes sencillos de texto. Desde hace algunos años, ha surgido la demanda de distribuir correo con capacidad de contener distintos tipos de datos, incluyendo voz, imágenes y secuencias de vídeo. Para satisfacer estos requisitos se ha definido un nuevo estándar sobre la base de SMTP: las extensiones multipropósito de correo electrónico (MIME, *Multi-Purpose Internet Mail Extension*). En esta sección estudiaremos primero SMTP y después MIME.

PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO (SMTP)

SMTP es el protocolo estándar para la transferencia de correo entre computadores en la familia de protocolos TCP/IP. SMTP está definido en el RFC 821.

Aunque los mensajes transferidos por SMTP normalmente siguen el formato definido en el RFC 822, que describiremos más adelante, a SMTP no le atañe ni el formato ni el contenido de los mensajes transferidos, con dos excepciones. Se hace referencia a este concepto diciendo que SMTP utiliza la información escrita en el *sobre* del correo (cabecera del mensaje), pero que no examina el contenido (cuerpo del mensaje) del sobre. Las dos excepciones son las siguientes:

1. SMTP normaliza el conjunto de caracteres del mensaje al conjunto ASCII de 7 bits.
2. SMTP incorpora información al comienzo del mensaje transferido que indica el camino que ha seguido el mismo.

Funcionamiento básico del correo electrónico

La Figura 22.1 muestra el flujo general del correo en un sistema típico. Aunque gran parte de esta actividad se encuentra fuera del ámbito de SMTP, la figura muestra el contexto dentro del que opera normalmente SMTP.

Para empezar, el correo lo crea un programa agente de usuario en respuesta a una entrada de usuario. Cada mensaje creado consta de una cabecera que incluye la dirección de correo electrónico del destinatario junto con otra información y un cuerpo que contiene el mensaje a enviar. Estos mensajes se sitúan de alguna forma en una cola de espera y se suministran como entrada a un programa emisor SMTP, que normalmente es un programa servidor siempre presente en el computador.

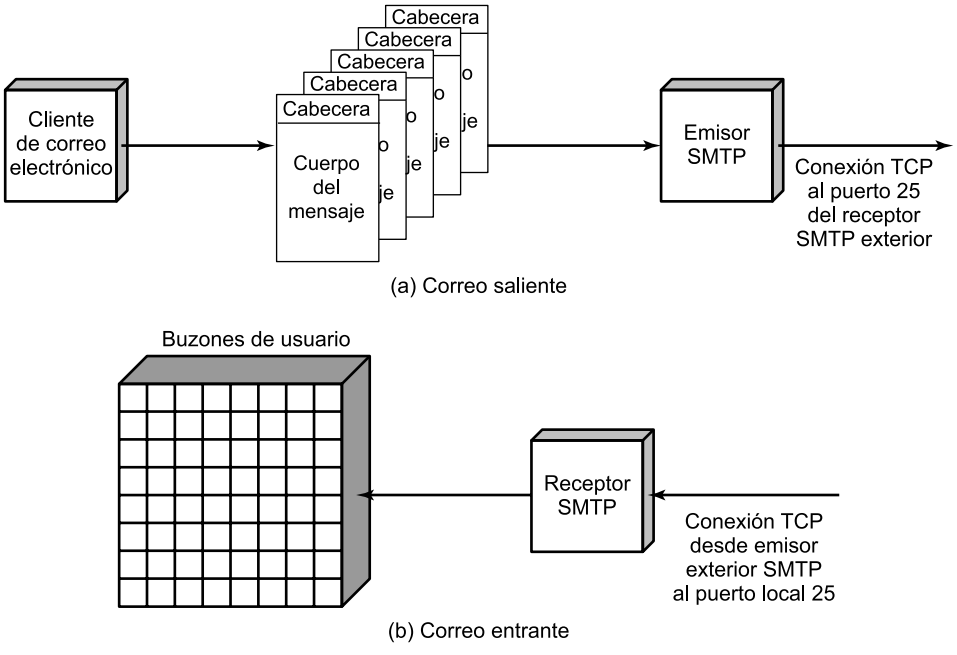

Cliente de correo electrónico
Cabecera
Cuerpo del mensaje
Emisor SMTP
Conexión TCP al puerto 25 del receptor SMTP exterior
(a) Correo saliente
Buzones de usuario
Receptor SMTP
Conexión TCP desde emisor exterior SMTP al puerto local 25
(b) Correo entrante

Figura 22.1. Flujo de correo SMTP.

Aunque la estructura de la cola de salida de correo será diferente según el sistema operativo del computador, cada mensaje en cola tiene conceptualmente dos partes:

1. El texto del mensaje, compuesto por:
   - La cabecera RFC 822: ésta constituye el sobre del mensaje e incluye una indicación del destinatario o destinatarios deseados.
   - El cuerpo del mensaje, escrito por el usuario.
2. Una lista de destinos de correo.

La lista de destinos de correo para los mensajes la obtiene el agente de usuario a partir de la cabecera RFC 822 del mensaje. En algunos casos, el destino o destinos se especifican literalmente en la cabecera del mensaje. En otros casos, el agente de usuario puede necesitar expandir los nombres de la lista de correo, eliminar duplicados y reemplazar nombres mnemónicos por los nombres de buzones de correo reales. Si se indica alguna copia de carbón oculta (BCC, *Blind Carbon Copy*), el agente de usuario necesita preparar mensajes para ajustarse a este requisito. La idea básica consiste en que los distintos formatos y estilos preferidos por los humanos en la interfaz de usuario se reemplacen por una lista normalizada adecuada para el programa de envío SMTP.

El **programa de envío SMTP** toma los mensajes de la cola de salida de correo y los transmite al computador destino adecuado mediante transacciones SMTP a través de una o más conexiones TCP al puerto 25 del computador objetivo. Un computador puede tener varios programas de envío SMTP activos simultáneamente si tiene una gran cantidad de volumen de correo de salida, y también debe tener la capacidad de crear receptores SMTP bajo demanda para que el correo que provenga de un computador no retarde el correo de otro.

Cuando el emisor SMTP completa la entrega de un mensaje específico a uno o más usuarios de un computador concreto, el emisor elimina los correspondientes destinatarios de la lista de destinos del mensaje. Cuando se han procesado todos los destinos de un mensaje concreto, éste se elimina de la cola. En el procesamiento de una cola, el emisor SMTP puede llevar a cabo varias optimizaciones. Si un mensaje determinado se envía a distintos usuarios de un único computador, sólo es necesario enviar el texto del mensaje una vez. Si hay listos para enviar varios mensajes al mismo computador, el emisor SMTP puede abrir una sola conexión TCP, transferir los múltiples mensajes y cerrar la conexión, en lugar de abrir y cerrar una conexión para cada mensaje.

El emisor SMTP debe hacer frente a diversos tipos de errores. El computador destino puede estar fuera de alcance, no encontrarse en funcionamiento o puede fallar la conexión TCP mientras se está transfiriendo el correo. El emisor puede volver a poner en cola el correo para efectuar la transferencia más tarde, pero renunciando a intentarlo otra vez tras un período de tiempo determinado en lugar de mantenerlo en la cola indefinidamente. Un error común consiste en indicar una dirección de destinatario errónea, debido a un error en la entrada del usuario o a que el destino deseado tiene una nueva dirección en un computador diferente. Si es posible, el emisor SMTP debe redirigir el mensaje o devolver una notificación de error al que originó el mensaje.

El **protocolo SMTP** se utiliza para transferir un mensaje desde el emisor SMTP al receptor SMTP a través de una conexión TCP. SMTP intenta proporcionar un funcionamiento fiable, pero no garantiza la recuperación de mensajes perdidos. No hay confirmación extremo a extremo de la entrega con éxito del mensaje para el que lo originó y tampoco se garantiza la notificación de los errores. Sin embargo, el sistema de correo basado en SMTP es generalmente considerado fiable.

El **receptor SMTP** acepta cada mensaje que llega y lo sitúa en el buzón de correo del usuario adecuado o lo copia en la cola local de correo de salida para reenviarlo si es necesario. El receptor

SMTP debe ser capaz de verificar los destinos locales de correo y atender los errores, incluyendo los errores de transmisión y de falta de espacio para almacenamiento.

El emisor SMTP es responsable del mensaje hasta el momento en el que el receptor SMTP indica que la transferencia se ha completado. Sin embargo, esto sólo significa que el mensaje ha llegado al receptor SMTP, no que el mensaje haya sido entregado y recogido por el destinatario final deseado. Las responsabilidades del receptor SMTP sobre al tratamiento de errores se restringen generalmente a abandonar conexiones TCP que fallen o que estén inactivas por largos períodos de tiempo. Por ello, la mayor parte de las responsabilidades en cuanto a la recuperación de los errores se sitúa en el emisor. Los errores que se produzcan durante la indicación de la finalización pueden producir la duplicación de mensajes, pero no su pérdida.

En la mayoría de los casos, los mensajes van directamente desde la máquina que origina el mensaje hasta la máquina destino a través de una única conexión TCP. Sin embargo, el mensaje pasará ocasionalmente por máquinas intermedias mediante la capacidad de reenvío de SMTP, en cuyo caso el mensaje debe atravesar una sucesión de conexiones TCP entre la fuente y el destino. Uno de los casos en que esto se produce consiste en que el emisor especifique una ruta al destino mediante una secuencia de servidores. Un caso más usual es el del reenvío requerido debido al traslado de un usuario.

Es importante señalar que el protocolo SMTP se limita a la conversación que tiene lugar entre el emisor SMTP y el receptor SMTP. La función principal de SMTP es la transferencia de mensajes, aunque existan algunas funciones auxiliares para la verificación y procesado del destino del correo. El resto del sistema de tratamiento de correo mostrado en la Figura 22.1 está fuera del ámbito de SMTP y puede diferir de un sistema a otro.

Volvamos a una discusión de los elementos principales de SMTP.

Visión general de SMTP

El funcionamiento de SMTP consiste en una serie de órdenes y respuestas intercambiadas entre el emisor y receptor SMTP. La iniciativa la lleva el SMTP emisor, quien establece la conexión TCP. Una vez que se ha establecido la conexión, el emisor SMTP envía órdenes al receptor a través de la conexión. Cada orden genera exactamente una respuesta del receptor SMTP.

La Tabla 22.1 muestra las **órdenes SMTP**. Cada orden consta de una única línea de texto que comienza con un código de orden de 4 letras, seguido en algunos casos por un campo de argumento. La mayoría de las repuestas constan de una sola línea, aunque son posibles respuestas de varias líneas. En la tabla se señalan aquellas órdenes que todos los receptores deben ser capaces de reconocer. Las otras órdenes son opcionales y pueden ser ignoradas por el receptor.

Las **respuestas SMTP** se muestran en la Tabla 22.2. Cada respuesta comienza con un código de tres dígitos, pudiendo ir seguida por información adicional. El primer dígito indica la categoría de la respuesta:

- **Respuesta de finalización positiva:** la acción solicitada se ha completado satisfactoriamente. Puede iniciarse una nueva solicitud.
- **Respuesta intermedia positiva:** la orden ha sido aceptada, pero la acción solicitada se encuentra suspendida, pendiente de la recepción de información adicional. El emisor SMTP debe enviar otra orden especificando está información. Esta respuesta se utiliza en grupos de secuencias de órdenes.

Tabla 22.1. Órdenes SMTP.

Nombre	Formato de la orden	Descripción
HELO	HELO ⟨SP⟩ ⟨dominio⟩ ⟨CRLF⟩	Envía identificación
MAIL	MAIL ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Identifica al que origina el correo
RCPT	RCPT ⟨SP⟩ TO: ⟨camino al destino⟩ ⟨CRLF⟩	Identifica al destinatario del correo
DATA	DATA ⟨CRLF⟩	Transfiere el texto del mensaje
RSET	RSET ⟨CRLF⟩	Aborta la transacción del correo en curso
NOOP	NOOP ⟨CRLF⟩	Operación nula
QUIT	QUIT ⟨CRLF⟩	Cierra la conexión TCP
SEND	SEND ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Envía correo al terminal
SOML	SOML ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Envía correo al terminal si es posible. En caso contrario, lo envía al buzón
SAML	SAML ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Envía correo al terminal y al buzón
VRFY	VRFY ⟨SP⟩ ⟨cadena⟩ ⟨CRLF⟩	Confirma el nombre del usuario
EXPN	EXPN ⟨SP⟩ ⟨cadena⟩ ⟨CRLF⟩	Devuelve la lista de miembros de una lista de correo
HELP	HELP [⟨SP⟩ ⟨cadena⟩] ⟨CRLF⟩	Envía documentación específica del sistema
TURN	TURN ⟨CRLF⟩	Intercambia el rol del emisor y el receptor

⟨CRLF⟩ = retorno de carro, salto de línea
⟨SP⟩ = espacio
Los corchetes indican elementos opcionales.
Los comandos sombreados son opcionales en implementaciones conformes a SMTP.

- **Respuesta de finalización negativa transitoria:** la orden no se aceptó y la acción solicitada no se llevó a cabo. Sin embargo, la condición de error es temporal y puede solicitarse la acción de nuevo.
- **Respuesta de finalización negativa permanente:** la orden no se aceptó y la acción solicitada no se realizó.

La operación básica de SMTP se produce en tres fases: establecimiento de la conexión, intercambio de uno o más pares orden-respuesta y cierre de la conexión. A continuación, se examina cada una de las fases.

Establecimiento de la conexión

Un emisor SMTP intentará establecer una conexión TCP con un computador destino cuando tenga uno o más mensajes de correo para entregarle. La secuencia es bastante sencilla:

1. El emisor abre una conexión TCP con el receptor.
2. Una vez que se ha establecido la conexión, el receptor se identifica a sí mismo con la respuesta «220 servicio preparado».
3. El emisor se identifica a sí mismo con la orden *HELO*.
4. El receptor acepta la identificación del emisor mediante la respuesta «250 OK».

Tabla 22.2. Respuestas SMTP.

Código	Descripción
Respuesta de finalización positiva	
211	Estado del sistema o respuesta de ayuda del sistema.
214	Mensaje de ayuda. (Información de cómo utilizar el receptor o el significado de una orden particular no estándar. Esta respuesta es sólo útil al usuario humano)
220	⟨dominio⟩ Servicio preparado
221	⟨dominio⟩ Servicio cerrando el canal de transmisión
250	Acción de correo solicitada correcta, completada
251	Usuario no local. Se reenviará a ⟨camino al destino⟩
Respuesta intermedia positiva	
354	Comenzar el texto del correo. Acabar con ⟨CRLF⟩.⟨CRLF⟩
Respuesta de finalización negativa transitoria	
421	⟨dominio⟩ Servicio no disponible; perdiendo canal de transmisión (ésta puede ser la respuesta a cualquier orden si el servicio sabe que debe apagarse)
450	Acción de correo solicitada no ejecutada; buzón de correo no disponible (por ejemplo, buzón ocupado)
451	Cancelada acción solicitada; error local en el procesamiento
452	Acción solicitada no ejecutada; almacenamiento del sistema insuficiente
Respuesta de finalización negativa permanente	
500	Error de sintaxis; orden no reconocida (esto puede incluir errores, como línea de orden demasiado larga)
501	Error de sintaxis en los parámetros o los argumentos
502	Orden no implementada
503	Secuencia de órdenes incorrecta
504	Parámetro de orden no implementado
550	Acción solicitada no ejecutada; buzón de correo no disponible (por ejemplo, buzón no encontrado o no se accedió)
551	Usuario no local, por favor, pruebe con ⟨camino al destino⟩
552	Acción de correo solicitada cancelada; excedida la asignación de espacio de almacenamiento
553	Acción solicitada no ejecutada; nombre del buzón de correo no permitido (por ejemplo, sintaxis de correo incorrecta)
554	Transacción fallida

Si el servicio de correo no está disponible en el destino, el computador destino devuelve la respuesta «421 servicio no disponible» en el paso 2 y finaliza el proceso.

Transferencia de correo

Una vez que se ha establecido una conexión, el emisor SMTP puede enviar uno o más mensajes al receptor SMTP. Existen tres fases lógicas en la transferencia de un mensaje:

1. Una orden *MAIL* identifica al que originó el mensaje.
2. Una o más órdenes *RCPT* identifican a los destinatarios de este mensaje.
3. Una orden *DATA* transfiere el texto del mensaje.

La **orden *MAIL*** proporciona el camino inverso, que puede utilizarse para informar de errores. Si el receptor está preparado para aceptar mensajes de esta fuente, entonces devuelve una respuesta «250 OK». En otro caso devuelve una respuesta indicando un fallo al ejecutar la orden (códigos 451, 452, 552) o un error en la orden (códigos 421, 500 y 501).

La **orden *RCPT*** identifica a un destinatario individual de los datos del correo. Se puede especificar varios destinatarios mediante el uso múltiple de esta orden. Se devuelve una respuesta distinta por cada orden *RCPT*, con una de las siguientes posibilidades:

1. El receptor acepta el destinatario con una respuesta «250». Esto indica que el buzón de correo designado se encuentra en el sistema del receptor.
2. El destino necesitará el reenvío del correo que será efectuado por el receptor (251).
3. El destino requerirá una operación de reenvío, pero el receptor no lo reenviará. El emisor debe volver a enviarlo a la dirección de reenvío (551).
4. No existe un buzón de correo en este computador para este destinatario (550).
5. Se rechaza el destino debido a algún fallo de ejecución (códigos 450, 451, 452 y 552 y 553) o a un error en la orden (códigos 421, 500, 501 y 503).

La ventaja de utilizar una fase separada para *RCPT* es que el emisor no enviará el mensaje hasta que esté seguro de que el receptor está dispuesto a recibirlo para al menos un destinatario, evitando de este modo la sobrecarga que constituye enviar un mensaje completo para averiguar que se desconoce al destinatario. Una vez que el receptor SMTP está de acuerdo en recibir el mensaje de correo para al menos un destinatario, el emisor SMTP utiliza la **orden *DATA*** para iniciar la transferencia del mensaje. Si el receptor SMTP sigue dispuesto a recibir el mensaje, devuelve una respuesta «354». En otro caso, el receptor devuelve una respuesta indicando que hubo un fallo al ejecutar la orden (códigos 451 o 554) o un error en la orden (códigos 421, 500, 501 o 503). Si se devuelve la respuesta «354», el emisor SMTP procede a enviar el mensaje sobre la conexión TCP en forma de una secuencia de líneas ASCII. El fin del mensaje se indica con una línea que contiene únicamente un punto («.»). El receptor SMTP responde con una respuesta «250 OK» si se acepta el mensaje o con el código de error apropiado (451, 452, 552 o 554) en caso contrario.

El siguiente ejemplo, tomado del RFC 821, muestra el proceso:

S:MAIL FROM: <Smith@Alpha.ARPA>
R: 250 OK

S:RCPT TO: <Jones@Beta.ARPA>
R: 250 OK

S:RCPT TO: <Green@Beta.ARPA>
R: 550 No such user here

S:RCPT TO: <Brown@Beta.ARPA>
R: 250 OK

S:DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>

S: Bla bla bla ...
S: ... etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK

El emisor SMTP está transmitiendo un correo creado por el usuario Smith@Alpha.ARPA. El mensaje va dirigido a tres usuarios en la máquina Beta.ARPA, llamados Jones, Green y Brown. El receptor SMTP indica que tiene buzones de correo para Jones y Brown, pero que no tiene información sobre Green. Ya que al menos uno de los destinatarios deseados ha sido verificado, el emisor procede a enviar el mensaje de texto.

Cierre de la conexión

El emisor SMTP cierra la conexión en dos pasos. Primero, el emisor envía una orden *QUIT* y espera una respuesta. El segundo paso consiste en iniciar una operación de cierre de la conexión TCP. El receptor inicia su cierre TCP después de enviar su respuesta a la orden *QUIT*.

RFC 822

El RFC 822 define un formato para los mensajes de texto que se envían utilizando el correo electrónico. El estándar SMTP adopta el RFC 822 como formato a utilizar en la construcción de mensajes para su transmisión a través de SMTP. En el contexto del RFC 822, los mensajes se componen de un sobre y un contenido. El sobre contiene toda la información necesaria para llevar a cabo la transmisión y la entrega. El contenido está compuesto por el objeto que ha de entregarse al destinatario. El estándar RFC 822 se aplica solamente al contenido. Sin embargo, el estándar del contenido incluye un conjunto de campos de cabecera que puede utilizar el sistema de correo para crear el sobre, con la finalidad de facilitar a los programas la adquisición de esa información.

Un mensaje RFC 822 consta de una secuencia de líneas de texto y utiliza una plantilla general. Es decir, un mensaje consta de varias líneas de cabecera que siguen un formato rígido, seguidas de una sección correspondiente al cuerpo compuesto por texto arbitrario.

Una línea de cabecera consta normalmente de una palabra clave, seguida por dos puntos («:») y los argumentos de la palabra clave. Este formato permite que una línea larga sea fragmentada en varias líneas. Las palabras clave más frecuentemente utilizadas son: «From» («de»), «To» («a»), «Subject» («asunto») y «Date» («fecha»). Aquí se muestra un ejemplo de mensaje:

Date: Tue, 16 Jan 1996 10:37:17 (EST)

From: «William Stallings» <ws@host.com>

Subject: La sintaxis en el RFC 822

To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hola. Esta parte constituye el comienzo real del cuerpo del mensaje, separado de la cabecera del mensaje por una linea[1] en blanco.

[1] *N. de T.:* se omiten las tildes ya que el RFC 822 únicamente acepta caracteres ASCII de 7 bits.>

Otro campo que se encuentra a menudo en la cabecera RFC 822 es «Message-ID» («identificador del mensaje»). Este campo contiene un identificador único asociado a este mensaje.

EXTENSIONES MULTIPROPÓSITO DE CORREO ELECTRÓNICO (MIME)

MIME es una extensión del marco de trabajo establecido en el RFC 822 que pretende abordar algunos de los problemas y limitaciones del uso de SMTP y del RFC 822 para el correo electrónico. [RODR02] señala las siguientes limitaciones del esquema SMTP/822:

1. SMTP no puede transmitir ficheros ejecutables u otros objetos binarios. Se utilizan diversos esquemas para convertir ficheros binarios a formato texto de forma que los sistemas de correo de SMTP puedan utilizarlos, incluyéndose el popular esquema de UNIX UUencode/UUdecode. Sin embargo, ninguno de estos procedimientos de conversión constituye un estándar, ni siquiera de facto.
2. SMTP no puede transmitir datos de texto que incluyan caracteres de lenguajes nacionales, ya que éstos se representan por códigos de 8 bits con valores de 128 en decimal o superiores, y SMTP está limitado a caracteres ASCII de 7 bits.
3. Los servidores SMTP pueden rechazar mensajes de correo que superen un cierto tamaño.
4. Las pasarelas de SMTP que traducen caracteres ASCII a código EBCDIC no utilizan un conjunto consistente de correspondencias, lo que da lugar a problemas en la traducción.
5. Las pasarelas de SMTP a redes de correo electrónico X.400 no pueden manejar los datos no textuales incluidos en mensajes X.400.
6. Algunas implementaciones no se adhieren completamente al estándar de SMTP definido en el RFC 821. Éstos son algunos de los problemas comunes que aparecen:
   - La eliminación, incorporación o reordenación de caracteres retorno de carro y de salto de línea.
   - El truncado o el solapamiento de las líneas de longitud mayor a 76 caracteres.
   - La eliminación de espacios en blanco finales (caracteres tabuladores y espacios).
   - El completado de las líneas de un mensaje para conseguir la misma longitud en todas.
   - La conversión de los caracteres tabuladores en varios caracteres de espacio.

MIME pretende resolver estos problemas de forma que resulte compatible con las implementaciones existentes del RFC 822. La especificación se encuentra en los RFC del 2045 al 2049.

Visión general

La especificación de MIME incluye los siguientes elementos:

1. Se definen cinco campos nuevos de la cabecera del mensaje, los cuales pueden incluirse en una cabecera RFC 822. Estos campos proporcionan información acerca del cuerpo del mensaje.
2. Se definen varios formatos para el contenido, normalizando así las representaciones que dan soporte al correo electrónico multimedia.
3. Se definen esquemas de codificación de transferencia, posibilitando así la conversión de cualquier formato de contenido a un formato protegido contra las alteraciones que efectúe el sistema de correo.

En esta subsección presentamos los cinco nuevos campos de la cabecera del mensaje. En las dos siguientes se examinan los formatos de contenido y los esquemas de codificación de transferencia. Los cinco campos de cabecera definidos en MIME son:

- ***M*IME-Version («versión de MIME»):** el valor de parámetro debe ser «1.0». Este campo indica que el mensaje cumple los RFC.
- ***Content-Type* («tipo de contenido»):** describe los datos contenidos en el cuerpo del mensaje con suficiente detalle, de tal manera que el agente de usuario receptor pueda escoger un agente o un mecanismo apropiado para presentar los datos al usuario o, en otro caso, ocuparse de los datos de forma adecuada.
- ***Content-Transfer-Encoding* («esquema de codificación de transferencia del contenido»):** indica el tipo de transformación que se ha utilizado para representar el cuerpo del mensaje de modo que sea aceptable para el transporte del correo.
- ***Content-ID* («identificador del contenido»):** utilizado para identificar de forma unívoca entidades MIME en múltiples contextos.
- ***Content-Description* («descripción del contenido»):** una descripción en texto nativo del objeto incluido en el cuerpo. Esto es útil cuando el objeto no se puede visualizar (por ejemplo, datos de audio).

En una cabecera RFC 822 normal pueden aparecer todos o alguno de estos campos. Una implementación conforme debe permitir los campos *MIME-Version*, *Content-Type* y *Content-Transfer-Encoding*. Los campos *Content-ID* y *Content-Description* son opcionales y pueden ser ignorados por la implementación del destinatario.

Tipos de contenido MIME

El grueso de la especificación de MIME está relacionado con la definición de varios tipos de contenidos. Esto refleja la necesidad de proporcionar formas normalizadas de tratar una gran variedad de representaciones de información en un entorno multimedia.

La Tabla 22.3 enumera los tipos de contenido. Existen siete tipos de contenidos principales diferentes y un total de 14 subtipos. En general, un tipo de contenido declara el tipo general de los datos y el subtipo especifica un formato particular para ese tipo de datos.

Para un cuerpo del **tipo *text* («texto»),** no se requiere un software especial para obtener el significado completo del texto, aparte de soportar el conjunto de caracteres indicado. El único subtipo definido es el texto nativo, que consiste simplemente en una cadena de caracteres ASCII o caracteres ISO 8859. Una versión anterior de la especificación MIME incluía el subtipo *richtext* (*texto enriquecido*), que admite una mayor flexibilidad en el formateo. Se espera que este subtipo vuelva a aparecer en un RFC posterior.

El **tipo *multipart* («multiparte»)** indica que el cuerpo del mensaje contiene múltiples partes independientes. El campo *Content-Type* de la cabecera incluye un parámetro, llamado delimitador, que define la marca utilizada para delimitar las distintas partes del cuerpo. Este delimitador no debe aparecer en ninguna de las partes del mensaje. Cada límite comienza en una línea nueva y consta de dos guiones seguidos por el valor del delimitador. El delimitador final, que indica el fin de la última parte, tiene además dos guiones como sufijo. Dentro de cada parte puede existir una cabecera opcional MIME ordinaria.

Tabla 22.3. Tipos de contenido MIME.

Tipo	Subtipo	Descripción
Texto	Nativo	Texto no formateado; puede ser ASCII o ISO 8859
Multipart («multiparte»)	*Mixed* («mixto»)	Las diferentes partes son independientes pero van a ser transmitidas juntas. Se deben presentar al receptor en el mismo orden en que aparecen en el mensaje de correo.
	Parallel («paralelo»)	Difiere del subtipo *mixed* solamente en que no se define orden para la entrega de las partes al receptor.
	Alternative («Alternativo»)	Las diferentes partes son versiones alternativas de la misma información. Están ordenadas en fidelidad creciente al original y el sistema de correo destino debe mostrar la mejor versión para el usuario.
	Digest («resumen»)	Similar al subtipo *mixed*, pero el tipo/subtipo por defecto para cada parte es message/rfc822.
Message («mensaje»)	rfc822	El propio cuerpo es un mensaje encapsulado que cumple con el RFC 822.
	Partial («parcial»)	Utilizado para permitir la fragmentación de elementos de correo grandes de forma que sea transparente al destino.
	External-body («cuerpo-externo»)	Contiene un puntero a un objeto que existe en otra parte.
Image («Imagen»)	jpeg	La imagen está en formato JPEG, codificación JFIF.
	gif	La imagen está en formato GIF.
Video («Vídeo»)	mpeg	Formato MPEG.
Audio	*Basic* («Básico»)	Codificación en ley-*mu* de RDSI, con un canal de 8 bits.
Application («aplicación»)	*Postscript*	Postscript de Adobe.
	octet-stream («flujo de octetos»)	Datos binarios generales compuestos por bytes de 8 bits.

A continuación, se muestra un ejemplo de mensaje multiparte, que contiene dos partes, cada una compuesta por texto simple:

From: John Smith <js@company.com>
To: Ned Jones <ned@soft.com>
Subject: Mensaje de muestra
MIME-Version: 1.0
Content-type: multipart/mixed; boundary = «delimitador simple»

Esto es el preambulo. Va a ser ignorado, aunque es un buen lugar para que los que componen el correo incluyan una nota explicativa para los lectores que no admitan MIME.

– delimitador simple

Esto es implicitamente texto de tipo ASCII. No termina con una ruptura de linea

– delimitador simple
Content-type: text/plain; charset = us-ascii

Esto es explicitamente texto de tipo ASCII. Termina con una ruptura de linea.

– delimitador simple –
Este es el epilogo. Va a ser ignorado.

Existen cuatro subtipos del tipo multiparte, todos con la misma sintaxis general. El **subtipo *multipart/mixed* («multiparte/mixto»)** se utiliza cuando existen múltiples partes de cuerpo independientes que necesitan disponerse en un orden particular. Para el subtipo ***multipart/parallel*** **(«multiparte/paralelo»)**, el orden de las partes no es significativo. Si el sistema del destinatario es apropiado, las múltiples partes pueden presentarse en paralelo. Por ejemplo, una parte de texto o de imagen se podría acompañar por un comentario verbal que se reproduce cuando se muestra el texto o la imagen.

Para el ***subtipo multipart/alternative*** **(«multiparte/alternativo»)**, las distintas partes constituyen representaciones diferentes de la misma información. Por ejemplo:

From: John Smith <js@company.com>
To: Ned Jones <ned@soft.com>
Subject: Correo de texto formateado
MIME-Version: 1.0
Content-type: multipart/alternative; boundary = «delimita42»
– delimita42

Content-type: text/plain; charset = us-ascii

... el mensaje en texto nativo va en esta parte...
– delimita42
Content-type: text/richtext

... el mismo mensaje en texto enriquecido RFC 1341 va en esta parte
– delimita42 –

En este subtipo, las partes del cuerpo están dispuestas en orden de preferencia creciente. En este ejemplo, si el sistema destinatario es capaz de mostrar el mensaje en forma de texto enriquecido, lo muestra. En caso contrario se utiliza el formato de texto nativo.

El ***subtipo multipart/digest*** **(«multiparte/resumen»)** se utiliza cuando cada parte del cuerpo se interpreta como un mensaje RFC 822 con cabeceras. Este subtipo permite la construcción de un mensaje cuyas partes sean mensajes individuales. Por ejemplo, el moderador de un grupo podría reunir mensajes de correo electrónico de los participantes, agrupar estos mensajes y enviarlos encapsulados en un mensaje MIME.

El **tipo *message*** **(«mensaje»)** proporciona a MIME una serie de capacidades importantes. El **subtipo *message/rfc822*** **(«mensaje/rfc822»)** indica que el cuerpo es un mensaje completo, incluyendo cabecera y cuerpo. A pesar del nombre de este subtipo, el mensaje encapsulado puede no ser un mensaje RFC 822 simple, sino cualquier mensaje MIME.

El **subtipo *message/partial*** **(«mensaje/parcial»)** permite la fragmentación de un mensaje largo en varias partes, que deben reensamblarse en el destinatario. Para este subtipo se especifican tres parámetros en el campo *Content-Type*:*Message*/*Partial*:

Identificador: un valor que es común a cada fragmento del mismo mensaje, de forma que se puedan identificar en el destino para poder reensamblarlos, pero que es único entre mensajes diferentes.

Número: un número de secuencia que indica la posición del fragmento en el mensaje original. El primer fragmento se numera como 1, el segundo como 2 y así sucesivamente.

Total: el número total de partes. El último fragmento se identifica por tener el mismo valor en los parámetros *número* y *total*.

El **subtipo *message/external-body* («mensaje/cuerpo externo»)** indica que los datos reales que se van a transferir en este mensaje no están contenidos en el cuerpo. En lugar de eso, el cuerpo contiene la información necesaria para acceder a los datos. Como con otros tipos de mensaje, el subtipo *message*/*external-body* tiene una cabecera externa y un mensaje encapsulado con su propia cabecera. El único campo necesario en la cabecera externa es el campo *Content-Type*, que identifica este mensaje como del subtipo *message*/*external-body*. La cabecera interna es la cabecera del mensaje encapsulado.

El campo *Content-Type* de la cabecera exterior debe incluir un parámetro de tipo de acceso, que tiene uno de los siguientes valores:

- **FTP:** el cuerpo del mensaje se encuentra accesible como un fichero, utilizando el protocolo de transferencia de ficheros (FTP). Para este tipo de acceso, son obligatorios los siguientes parámetros adicionales: nombre (el nombre del fichero) y localización (nombre de dominio del computador donde reside el fichero). Los parámetros opcionales son: directorio (el directorio donde se sitúa el fichero) y modo (que indica la forma en que FTP debe recuperar el fichero, por ejemplo, como ASCII o imagen). Antes de que tenga lugar la transferencia, el usuario necesitará proporcionar un identificador y una contraseña de usuario. Estos no se transmiten con el mensaje por razones de seguridad.
- **TFTP:** el cuerpo del mensaje está accesible como fichero mediante el protocolo trivial de transferencia de ficheros (TFTP). Se utilizan los mismos parámetros que para FTP y, de igual forma, se ha de proporcionar un identificador y una contraseña de usuario.
- **Anon-FTP («FTP anónimo»):** es idéntico a FTP, exceptuando que no se solicita el identificador y la contraseña del usuario. El parámetro nombre proporciona el nombre del fichero.
- **local-file («fichero local»):** el cuerpo del mensaje se encuentra accesible como un fichero en la máquina destino.
- **AFS:** el cuerpo del mensaje está accesible como un fichero a través del AFS (*Andrew File System*) global. El parámetro nombre proporciona el nombre del fichero.
- **mail-server («servidor de correo»):** al cuerpo del mensaje se accede enviando un mensaje de correo electrónico a un servidor de correo. Se debe incluir el parámetro *servidor* para dar la dirección de correo electrónico del servidor. El cuerpo del mensaje original, conocido como «cuerpo fantasma», debería contener la orden exacta que se ha de enviar al servidor de correo.

El **tipo *image* («imagen»)** indica que el cuerpo contiene una imagen que se puede visualizar. El subtipo, jpeg o gif, especifica el formato de la imagen. En el futuro se incorporarán más subtipos a esta lista.

El **tipo *video* («vídeo»)** indica que el cuerpo contiene una imagen que varía en el tiempo, posiblemente con color y sonido coordinado. El único subtipo especificado hasta ahora es mpeg.

El **tipo *audio* («audio»)** indica que el cuerpo contiene datos de audio. El único subtipo, básico, se ajusta a un servicio RDSI conocido como «64 kbps, estructurado a 8 kHz, utilizable para información de voz», con un algoritmo de digitalización de voz conocido como PCM ley-μ. Este tipo general constituye la forma usual de transmitir señales de voz a través de una red digital. El término *ley*-μ se refiere a una técnica de codificación estándar que se utiliza en América del Norte y Japón. En Europa se utiliza el sistema estándar rival, denominado ley-A.

El **tipo *application* («aplicación»)** se refiere a otros tipos de datos, normalmente datos binarios sin interpretación o información que se ha de procesar por una aplicación basada en correo. El **subtipo *application/octet-stream* («aplicación/flujo de octetos»)** indica datos binarios generales

en forma de secuencia de octetos. El RFC 2045 recomienda que la implementación del receptor ofrezca almacenar los datos en un fichero o utilizarlos como entrada a un programa.

El **subtipo *application/Postscript* («aplicación/Postscript»)** indica el uso de Postscript de Adobe.

Esquemas de codificación de transferencia de MIME

El otro componente principal de la especificación MIME, además de la especificación del tipo de contenido, es la definición de la codificación de transferencia de los cuerpos de los mensajes. Su objetivo es proporcionar una entrega fiable a través del mayor número de entornos diversos.

El estándar MIME define dos métodos para codificar los datos. El campo *Content-Transfer-Encoding* en realidad puede tomar seis valores, como se muestra en la Tabla 22.4. Sin embargo, tres de estos valores (7bit, 8bit y binary) indican que no se ha efectuado ninguna codificación, pero en cambio proporcionan información sobre la naturaleza de los datos. Para la transferencia SMTP, es seguro utilizar la forma 7bit. Las formas 8bit y binary se pueden utilizar en otros contextos de transporte de correo. Otro valor de esquema de codificación de contenido es *x-token* («esquema x»), que indica que se utiliza algún otro esquema de codificación del que se proporcionará el nombre. Éste podría ser un esquema específico de un fabricante o de una aplicación concreta. Los dos esquemas de codificación reales definidos son el *quoted-printable* («imprimible textualmente») y el base64. Los dos esquemas se definen para ofrecer la posibilidad de escoger entre una técnica de transferencia que es esencialmente legible por humanos y otra que es segura para todos los tipos de datos en una forma razonablemente compacta.

Tabla 22.4. Esquemas de codificación de transferencia de MIME.

7bit	Todos los datos se representan por líneas cortas de caracteres ASCII.
8bit	Las líneas son cortas, pero puede haber caracteres no ASCII (octetos con el bit de orden más alto establecido).
Binary («binario»)	Además de incluir caracteres no ASCII, las líneas pueden no ser lo suficientemente cortas para el transporte SMTP.
quoted-printable («imprimible textualmente»)	Codifica los datos de tal forma que si la mayoría de los datos que se codifican son texto ASCII, el texto codificado permanece en gran medida reconocible por los usuarios humanos.
base64	Codifica los datos convirtiendo bloques de 6 bits en bloques de 8 bits, todos ellos caracteres ASCII imprimibles.
x-token («esquema x»)	Una codificación no estándar.

La codificación de transferencia **quoted-printable** es útil cuando los datos son en buena parte octetos que corresponden a caracteres ASCII imprimibles. En esencia, representa caracteres no seguros por medio de la representación en hexadecimal de sus códigos e introduce rupturas de líneas reversibles (auxiliares) para limitar la longitud de las líneas del mensaje a 76 caracteres. Las reglas de codificación son las siguientes:

1. Representación general de 8 bits: esta regla se va a utilizar cuando no se aplique ninguna de las otras reglas. Cualquier carácter se representa por un signo igual seguido de una representación en hexadecimal de dos dígitos del valor del octeto. Por ejemplo, el carácter de

salto de página ASCII, que tiene un valor en decimal de 8 bits de «12», se representa por «=0C».

2. Representación literal: cualquier carácter en el rango decimal comprendido entre 33 («!») y 126 («~»), exceptuando el decimal 61 («=»), se representa por el propio carácter ASCII.
3. Espacio en blanco: los octetos con valor 9 y 32 se pueden representar como los caracteres ASCII de tabulador y espacio respectivamente, excepto al final de la línea. Cualquier espacio en blanco (tabulador o espacio) al final de una línea se debe representar según la regla 1. Al decodificar se suprime cualquier espacio en blanco al final de la línea. Esto elimina cualquier espacio en blanco incorporado por agentes de transporte intermedios.
4. Ruptura de línea: cualquier ruptura de línea, independientemente de su representación inicial, se representa por la ruptura de línea del RFC 822, que consiste en la combinación de un retorno de carro y un salto de línea (<CRLF>).
5. Ruptura de línea reversible: si una línea codificada va a tener una longitud mayor que 76 caracteres (excluyendo <CRLF>), se debe insertar una ruptura de línea reversible antes de la posición 76. Una ruptura de línea reversible consiste en la secuencia en hexadecimal 3D0D0A, que es el código ASCII para el signo igual seguido del retorno de carro y el salto de línea.

La **codificación de transferencia base64**, también conocida como codificación radix-64, es una técnica común para codificar datos binarios arbitrarios de forma que sean invulnerables al procesamiento de los programas de transporte de correo. Esta técnica convierte una entrada binaria arbitraria en una salida de caracteres imprimibles. Esta forma de codificación tiene las siguientes características relevantes:

1. El rango de la función es un conjunto de caracteres representable universalmente en todos los sitios, no una codificación binaria específica de ese conjunto de caracteres. Así, los propios caracteres se pueden codificar en cualquier forma que sea necesaria por un sistema determinado. Por ejemplo, el carácter «E» se representa en un sistema basado en ASCII por el valor hexadecimal 45 y en un sistema basado en EBCDIC por el valor hexadecimal C5.
2. El conjunto de caracteres consta de los 65 caracteres imprimibles, uno de los cuales se utiliza para el relleno. Con $2^6 = 64$ caracteres disponibles, cada carácter se puede utilizar para representar 6 bits de entrada.
3. No se incluyen caracteres de control en el conjunto. Así, un mensaje codificado en base64 puede atravesar sistemas de tratamiento de correo que comprueben el flujo de datos para encontrar caracteres de control.
4. El carácter de guión («-») no se utiliza. Este carácter tiene significado en el formato RFC 822, por lo que debe evitarse.

La Tabla 22.5 muestra la equivalencia de los valores de 6 bits de entrada con los caracteres. El conjunto de caracteres consta de los caracteres alfanuméricos más «+» y «/». El carácter «=» se utiliza como carácter de relleno.

La Figura 22.2 muestra un esquema de conversión sencillo. La entrada binaria se procesa en bloques de 3 octetos o 24 bits. Cada conjunto de 6 bits del bloque de 24 bits se convierte en un carácter. En la figura, los caracteres se muestran codificados como valores de 8 bits. En este caso típico, cada entrada de 24 bits se expande en una salida de 32 bits.

Tabla 22.5. Esquema de codificación radix-64.

Valor de 6 bits	Codificación del carácter	Valor de 6 bits	Codificación del carácter	Valor de 6 bits	Codificación del carácter	Valor de 6 bits	Codificación del carácter
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(relleno)	=

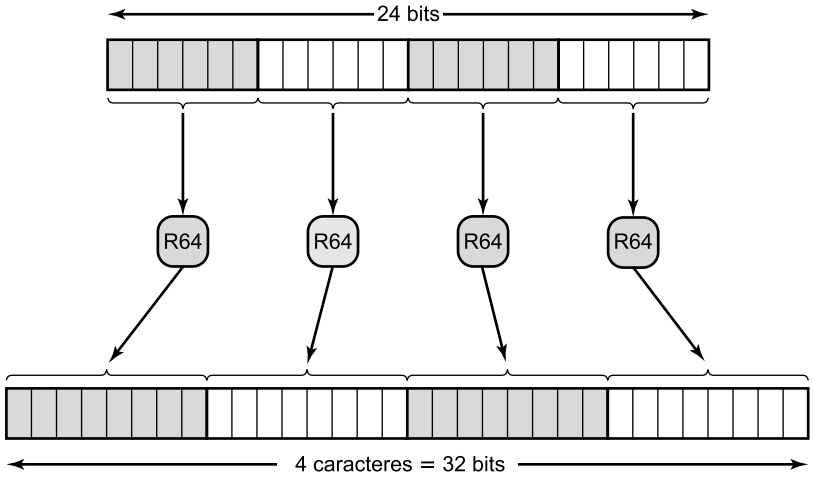


Figura 22.2. Correspondencia de la codificación imprimible de datos binarios con el formato radix-64.

Por ejemplo, considere la secuencia de texto original de 24 bits 00100011 01011100 10010001, que puede expresarse en hexadecimal como 235C91. Ordenando esta entrada en bloques de 6 bits se obtiene:

001000 110101 110010 010001

Los valores decimales de 6 bits extraídos son 8, 53, 50 y 17. Consultando estos valores en la Tabla 22.5 se obtienen los siguientes caracteres con codificación radix-64: I1yR. Si estos caracteres se almacenan en formato ASCII de 8 bits con el bit de paridad a cero, se tiene

01001001 00110001 01111001 01010010

En hexadecimal se expresa como 49317952. Para resumir:

Datos de entrada	
Representación binaria	00100011 01011100 10010001
Representación hexadecimal	235C91
Codificación radix-64 de los datos de entrada	
Representación en caracteres	I1yR
Código ASCII (8 bits paridad cero)	01001001 00110001 01111001 01010010
Representación hexadecimal	49317952

22.2. PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO (HTTP)

El protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*) es el protocolo base de la telaraña mundial (WWW, *World Wide Web*) y puede utilizarse en cualquier aplicación cliente-servidor que suponga la utilización de hipertextos. El nombre es más bien confuso, ya que HTTP no es un protocolo para transferir hipertexto, sino un protocolo para transmitir información con la eficiencia necesaria para efectuar saltos de hipertexto. Los datos transferidos por el protocolo pueden ser texto nativo, hipertexto, audio, imágenes o cualquier información accesible a través de Internet.

Comenzaremos con una descripción general de los conceptos HTTP y su funcionamiento y después examinaremos algunos de sus detalles, basando nuestra discusión en la versión más reciente a incluir en la lista de estándares de Internet, HTTP 1.1 (RFC 2616). En la Tabla 22.6 se resumen algunos de los términos más importantes definidos en las especificaciones de HTTP. Éstos se irán presentando a medida que avance la discusión.

DESCRIPCIÓN GENERAL DE HTTP

HTTP es un protocolo cliente/servidor orientado a transacciones. El uso más habitual de HTTP se produce entre un navegador y un servidor web. Para proporcionar fiabilidad, HTTP hace uso de TCP. No obstante, HTTP es un protocolo «sin estados»: cada transacción se trata independientemente. Por consiguiente, una implementación típica creará una conexión nueva entre el cliente y el servidor para cada transacción y cerrará la conexión tan pronto como se complete la transacción, aunque la especificación no impone esta relación uno a uno entre la transacción y la duración de la conexión.

La naturaleza de protocolo sin estados de HTTP es la adecuada para su aplicación habitual. Una sesión normal de un usuario con un navegador web supone obtener una secuencia de páginas y documentos web. La secuencia se lleva a cabo idealmente de forma rápida y las localizaciones de las distintas páginas y documentos pueden encontrarse en varios servidores ampliamente distribuidos.

Otra característica importante de HTTP es que es flexible en cuanto a los formatos que puede manejar. Cuando un cliente emite una solicitud a un servidor, puede incluir una lista priorizada de formatos con los que puede operar, respondiendo el servidor con el formato adecuado. Por ejemplo, un navegador *lynx* no puede operar con imágenes, por lo que el servidor no necesita transmitir

Tabla 22.6. Términos clave relacionados con HTTP.

Caché Almacén local de mensajes de respuesta o el subsistema que controla el almacenamiento, recuperación y borrado de los mensajes. Una caché almacena respuestas apropiadas para reducir el tiempo de respuesta y el consumo de ancho de banda en peticiones equivalente futuras. Cualquier cliente o servidor puede incluir una caché, aunque un servidor no puede utilizarla cuando actúa como túnel.	**Servidor de origen** El servidor en el que reside un recurso dado o donde se va a crear el recurso.
Cliente Un programa de aplicación que establece conexiones con el propósito de enviar solicitudes.	**Representante** Un programa intermedio que actúa tanto como servidor y como cliente con objeto de hacer las peticiones en nombre de otros clientes. Las solicitudes se atienden internamente o pasándolas, a veces traduciéndolas, a otros servidores. Un representante debe interpretar y, si es necesario, reescribir el mensaje de solicitud antes de reenviarlo. Los representantes son utilizados a menudo como portales del lado del cliente para atravesar cortafuegos de red y como aplicaciones de apoyo para atender solicitudes mediante protocolos no implementados por el agente de usuario.
Conexión Un circuito virtual de la capa de transporte establecido entre dos programas de aplicación con el propósito de comunicarse.	**Recurso** Un objeto de datos o un servicio de red que puede ser identificado por una URL.
Entidad Una representación concreta o interpretación de un recurso de datos o una respuesta de un recurso de servicio, que puede estar incluido dentro de un mensaje de solicitud o respuesta. Una entidad consta de cabeceras de entidad y un cuerpo de entidad.	**Servidor** Un programa de aplicación que acepta conexiones para dar servicio a solicitudes mediante el envío de respuestas de vuelta.
Pasarela Un servidor que actúa como intermediario para otro servidor. A diferencia de un representante, una pasarela recibe peticiones como si fuera el servidor original del recurso solicitado. El cliente solicitante puede no ser consciente de que está comunicando con una pasarela. Las pasarelas se utilizan a menudo como portales del lado del servidor para atravesar cortafuegos de red y como traductores de protocolos para acceder a recursos en sistemas que no emplean HTTP.	**Túnel** Un programa intermedio que está actuando como un retransmisor ciego entre dos conexiones. Una vez que está activo, no se considera como una parte de la comunicación HTTP, aunque puede haber sido iniciado por una solicitud HTTP. Un túnel deja de existir cuando ambos extremos de las conexiones se cierran. Los túneles se utilizan cuando se necesite un portal y el intermediario no pueda, o no deba, interpretar la comunicación retransmitida.
Mensaje La unidad básica de la comunicación HTTP, consistente en una secuencia estructurada de octetos transmitidos a través de la conexión.	**Agente de usuario** El cliente que inicia una solicitud. Entre estos se incluyen los navegadores, editores, arañas y otras herramientas del usuario final.

ninguna imagen de las existentes en las páginas web. Esta disposición evita la transmisión de información innecesaria y proporciona la base para ampliar el conjunto de formatos con nuevas especificaciones estándares y propietarias.

La Figura 22.3 muestra tres ejemplos del funcionamiento de HTTP. El caso más sencillo es aquel en el que un *agente de usuario* establece una conexión directa con el servidor origen. El *agente de usuario* es el cliente que inicia la solicitud, como es el caso de un navegador web actuando de parte de un usuario final. El *servidor origen* es el servidor en el que se encuentra el

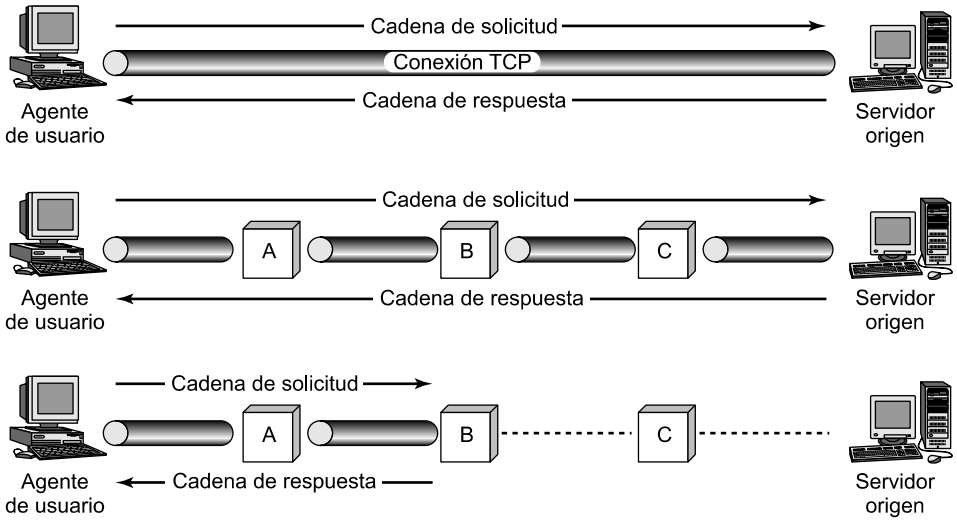


Figura 22.3. Ejemplos del funcionamiento de HTTP.

recurso de interés. Un ejemplo de esto lo constituye un servidor web en el que reside la página web de inicio deseada. Para este caso, el cliente abre una conexión TCP extremo a extremo entre el cliente y el servidor. El cliente emite entonces una solicitud HTTP. La solicitud consta de una orden concreta, denominada método, una URL y un mensaje de tipo MIME que contiene los parámetros de la solicitud, información acerca del cliente y, tal vez, alguna información adicional del contenido.

Cuando el servidor recibe la solicitud, intenta llevar a cabo la acción solicitada y después devuelve una respuesta HTTP. La respuesta incluye información de estado, un código de éxito o error y un mensaje de tipo MIME que contiene información sobre el servidor, información sobre la misma respuesta y un posible cuerpo con el contenido. A continuación, se cierra la conexión TCP.

En la parte central de la Figura 22.3 se muestra un caso en que no existe una conexión TCP extremo a extremo entre el agente de usuario y el servidor origen. En su lugar, existen uno o más sistemas intermedios con conexiones TCP entre sistemas lógicamente adyacentes. Cada sistema intermedio actúa como un retransmisor, de forma que una solicitud iniciada por el cliente se retransmite a través de los sistemas intermedios hasta el servidor y la respuesta del servidor se retransmite de vuelta al cliente.

Se definen tres tipos de sistemas intermedios en la especificación HTTP, ilustrados en la Figura 22.4: representante (*proxy*), pasarela (*gateway*) y túnel (*tunnel*).

Representante

Un representante actúa en nombre de otros clientes y presenta las solicitudes de éstos a un servidor. El representante actúa como servidor cuando interactúa con un cliente, y como cliente cuando interactúa con un servidor. Existen dos escenarios que requieren el uso de un representante:

- **Intermediario de seguridad:** el cliente y el servidor pueden estar separados por un intermediario de seguridad, como es el caso de un cortafuegos, con el representante en el lado del cliente. Normalmente, el cliente forma parte de una red protegida por un cortafuegos y el servidor es externo a esta red protegida. En este caso, el servidor se debe autenticar al corta-

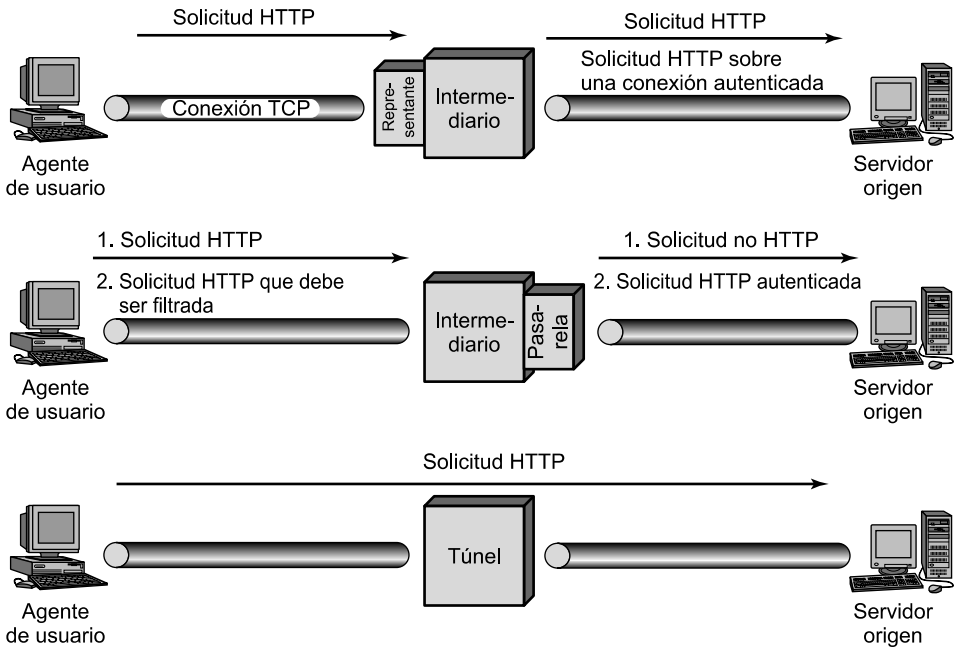


Figura 22.4. Sistemas HTTP intermediarios.

fuegos para establecer una conexión con el representante. El representante acepta respuestas después de haber atravesado el cortafuegos.

- **Diferentes versiones de HTTP:** si el cliente y el servidor ejecutan diferentes versiones de HTTP, el representante puede implementar ambas versiones y realizar las traducciones necesarias.

En resumen, un representante es un agente de reenvío que recibe solicitudes de objetos URL, modifica las solicitudes y las reenvía hacia el servidor identificado en la URL.

Pasarela

Una pasarela es un servidor que se presenta al cliente como si se tratase de un servidor origen. Actúa en nombre de otros servidores que no pueden comunicarse directamente con un cliente. Existen dos escenarios en los que se pueden utilizar pasarelas:

- **Intermediario de seguridad:** el cliente y el servidor pueden estar separados por un intermediario de seguridad, como es el caso de un cortafuegos, con la pasarela en el lado del servidor. Normalmente, el servidor está conectado a la red protegida por un cortafuegos y el cliente es externo a esta red. En este caso, el cliente se debe autenticar a la pasarela, que puede pasar entonces la solicitud al servidor.
- **Servidor no HTTP:** los navegadores web tienen incorporada la capacidad de contactar con servidores de otros protocolos distintos de HTTP, como servidores de FTP o Gopher. Esta capacidad también la puede proporcionar una pasarela. El cliente realiza una solicitud HTTP a un servidor pasarela. El servidor pasarela contacta con el servidor FTP o Gopher pertinente para obtener el resultado deseado. Este resultado se convierte entonces a un formato adecuado para HTTP y se transmite de vuelta al cliente.

Túnel

A diferencia del representante y la pasarela, el túnel no realiza operaciones sobre las solicitudes y respuestas HTTP. En su lugar, un túnel es simplemente un punto de retransmisión entre dos conexiones TCP y los mensajes HTTP se transfieren sin modificaciones, como si hubiera una única conexión HTTP entre el agente de usuario y el servidor origen. Los túneles se utilizan cuando deba existir un sistema intermediario entre el cliente y el servidor, pero no sea necesario para ese sistema comprender el contenido de los mensajes. Un ejemplo de este caso lo constituye un cortafuegos en el que un cliente o un servidor externo a la red protegida puede establecer una conexión autenticada y después mantener esa conexión con objeto de realizar las transacciones HTTP.

Caché

Volviendo a la Figura 22.3, su parte inferior muestra un ejemplo de una caché. Una caché es un servicio que puede almacenar solicitudes y respuestas previas para tratar las nuevas solicitudes. Si llega una solicitud nueva que es igual a una solicitud almacenada, entonces la caché puede proporcionar directamente la respuesta en lugar de acceder al recurso indicado en la URL. La caché puede operar en un cliente, en un servidor o en un sistema intermedio que no sea un túnel. En la figura, el intermediario B ha almacenado una transacción de solicitud/respuesta, de forma que para una nueva solicitud correspondiente del cliente no se necesite recorrer la cadena completa hasta el servidor origen, sino que se procese por B.

No todas las transacciones se pueden almacenar, pudiendo un cliente o un servidor indicar que ciertas transacciones pueden almacenarse sólo durante un determinado periodo de tiempo.

MENSAJES

La mejor forma de describir la funcionalidad de HTTP es describir los elementos individuales del mensaje HTTP. HTTP consta de dos tipos de mensajes: solicitudes de los clientes a los servidores y respuestas de los servidores a los clientes. La estructura general de estos mensajes se muestra en la Figura 22.5. Más formalmente, utilizando la notación BNF (*Backus-Naur Form*) (*véase* Tabla 22.7), tenemos:

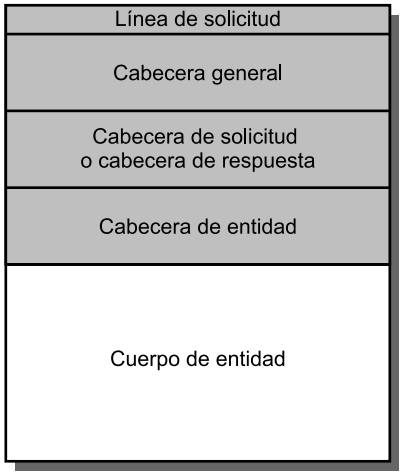


Figura 22.5. Estructura general de los mensajes HTTP.

Tabla 22.7. Notación BNF ampliada y utilizada en las especificaciones URL y HTTP

- Las palabras en minúsculas representan variables o nombres de reglas.
- Una regla tiene la forma

  nombre = definición

- DIGIT es cualquier dígito decimal; CRLF es el retorno de carro o salto de línea; SP representa uno o más espacios.
- Las comillas encierran texto literal
- Los ángulos «〈» «〉», se pueden utilizar dentro de una definición para delimitar un nombre en aras de una mayor claridad.
- Los elementos separados por una barra «|» son alternativos.
- Los paréntesis ordinarios se utilizan para agrupar.
- El carácter «*» que preceda a un elemento indica repetición. La forma completa es

  〈I〉*〈J〉elemento

  indicando al menos I y como mucho J ocurrencias del elemento. *elemento admite cualquier número de repeticiones, incluyendo 0; 1*elemento requiere al menos un elemento; 1*2elemento admite 1 o 2 elementos; 〈N〉elemento significa exactamente N elementos.
- Los corchetes «[» «]», encierran elementos opcionales.
- La construcción «≠» se utiliza para definir, con el siguiente formato:

  〈I〉≠〈J〉elemento

  indicando al menos I y como mucho J elementos, cada uno separado por una coma y espacios opcionales.
- Un punto y coma «;» a la derecha de una regla indica el comienzo de un comentario que continúa hasta el final de la línea.

```
HTTP-Message = Simple-Request | Simple-Response | Full-Request
| Full-Response
Full-Request = Request-Line
   *( General-Header | Request-Header | Entity-Header )
   CRLF
   [ Entity-Body ]
Full-Response = Status-Line
   *( General-Header | Response-Header | Entity-Header )
   CRLF
   [ Entity-Body ]
Simple-Request = "GET" SP Request-URL CRLF
Simple-Response = [ Entity-Body ]
```

Los mensajes «Simple-Request» y «Simple-Response» fueron definidos en HTTP/0.9. La solicitud consiste en una orden sencilla *GET* con la URL solicitada. La respuesta es simplemente un bloque que contiene la información identificada en la URL. En HTTP/1.1 se desaconseja la utilización de estos formatos simples, ya que impiden al cliente realizar la negociación del contenido y al servidor identificar el tipo de contenido de la entidad devuelta.

En las solicitudes y respuestas completas se utilizan los siguientes campos:

- ***Request-Line:*** identifica el tipo de mensaje y el recurso solicitado.
- ***Response-Line:*** proporciona información de estado sobre esta respuesta.
- ***General-Header:*** contiene campos aplicables a los mensajes de solicitud y de respuesta, pero que no se aplican a la entidad que está siendo transferida.
- ***Request-Header:*** contiene información acerca de la solicitud y el cliente.

- ***Response-Header:*** contiene información sobre la respuesta.
- ***Entity-Header:*** contiene información acerca del recurso identificado por la solicitud e información sobre el cuerpo de la entidad.
- ***Entity-Body:*** el cuerpo del mensaje.

Todas las cabeceras de HTTP constan de una secuencia de campos que siguen el mismo formato genérico que el RFC 822 (descrito en la Sección 22.1). Cada campo comienza en una línea nueva y se compone del nombre del campo seguido por dos puntos y el valor del campo.

Aunque el mecanismo básico de transacción es simple, existe un gran número de campos y parámetros definidos en HTTP. Éstos se muestran en la Tabla 22.8. En el resto de esta sección examinaremos los campos de la cabecera general. En las siguientes secciones se describirán las cabeceras de solicitud, las cabeceras de respuesta y las entidades.

Campos de la cabecera general

Los campos de la cabecera general pueden utilizarse en los mensajes de solicitud y de respuesta. Estos campos se aplican en ambos tipos de mensajes y contienen información que no se aplica directamente a la entidad que se está transfiriendo. Los campos son:

- ***Cache-Control*** **(«control de caché»):** especifica las directivas que ha de obedecer cualquier mecanismo que implemente una caché a lo largo de la cadena solicitud/respuesta. Su propósito es el de evitar que una caché interfiera de forma adversa sobre esta solicitud o respuesta concreta.
- ***Connection*** **(«conexión»):** contiene una lista de palabras clave y nombres de campos de cabecera que sólo se aplican a esta conexión TCP entre el emisor y el receptor más cercano que no sea un túnel.
- ***Date*** **(«Fecha»):** fecha y hora en la que se originó el mensaje.
- ***Forwarded*** **(«reenviado»):** utilizado por las pasarelas y representantes para indicar pasos intermedios a lo largo de la cadena de solicitud o respuesta. Cada pasarela o representante que procese un mensaje puede incorporar un campo «Forwarded» donde indique su URL.
- ***Keep-Alive*** **(«mantener activo»):** puede estar presente si existe la palabra clave «keep-alive» en un campo «Connection» recibido, para proporcionar información al solicitante sobre la conexión persistente. Este campo puede indicar la duración máxima que el emisor mantendrá abierta la conexión esperando la siguiente solicitud o el número máximo de solicitudes adicionales que se permitirán sobre la conexión persistente actual.
- ***MIME-Version*** **(«versión de MIME»):** indica que el mensaje cumple la especificación de la versión de MIME indicada.
- ***Pragma:*** contiene directivas específicas de implementación que pueden aplicarse a cualquier receptor a lo largo de la cadena de solicitud/respuesta.
- ***Upgrade*** **(«actualizar»):** se utiliza en una solicitud para especificar qué protocolos adicionales admite el cliente que querría utilizar. Se emplea en una respuesta para indicar qué protocolo será empleado.

MENSAJES DE SOLICITUD

Un mensaje de solicitud completo consta de una línea de estado seguida por una o más cabeceras generales de entidad y de solicitud, seguidas por un cuerpo de entidad opcional.

Tabla 22.8. Elementos de HTTP.

TODOS LOS MENSAJES	
Campos de la cabecera general	**Campos de la cabecera de entidad**
Cache-Control («control de caché») *Connection* («conexión») *Date* («fecha») *Forwarded* («reenviado») *Keep-Alive* («mantener activo») *MIME-Version* («versión de MIME») *Pragma* *Upgrade* («actualizar»)	*Allow* («admitir») *Content-Encoding* («esquema de codificación del contenido») *Content-Language* («lenguaje del contenido») *Content-length* («longitud del contenido») *Content-MD5* («MD5 del contenido») *Content-Range* («rango del contenido») *Content-Type* («tipo de contenido») *Content-Version* («versión del contenido») *Derived-From* («derivada de») *Expires* («expiración») *Last-Modified* («última modificación») *Link* («enlace») *Title* («título») *Transfer-Encoding* («esquema de codificación de transferencia») *URL-Header* («cabecera de URL») *Extension-header* («cabecera de extensión»)
MENSAJES DE SOLICITUD	
Métodos de solicitud	**Campos de la cabecera de solicitud**
OPTIONS («opciones») *GET* («obtener») *HEAD* («cabecera») *POST* («enviar») *PUT* («poner») *PATCH* («parchear») *COPY* («copiar») *MOVE* («mover») *DELETE* («eliminar») *LINK* («enlazar») *UNLINK* («desenlazar») *TRACE* («trazar») *WRAPPED* («empaquetado») *extension-method* («método de extensión»)	*Accept* («aceptar») *Accept-Charset* («aceptar conjunto de caracteres») *Accept-Encoding* («aceptar esquema de codificación») *Accept-Language* («aceptar lenguaje») *Authorization* («autorización») *From* («de») *Host* («computador») *if-Modified-Since* («si ha sido modificado desde») *Proxy-Authorization* («autorización del representante») *Range* («rango») *Referrer* («remitente») *Unless* («a menos que») *User-Agent* («agente de usuario»)
MENSAJES DE RESPUESTA	
Códigos de estado de respuesta	**Campos de la cabecera de respuesta**
Continue («continuar») *Switching Protocol* («cambiando de protocolo») *OK* («correcto») *Created* («creado») *Accepted* («aceptada») *Non-Authoritative Information* («información no acreditada») *No Content* («sin contenido») *Reset Content* («reiniciar contenido») *Partial Content* («contenido parcial») *Multiple Choices* («múltiples alternativas») *Moved Permanently* («trasladado permanentemente»)	*Location* («localización») *Proxy-Authenticate* («autenticación del representante») *Public* («Público») *Retry-After* («intentar después de») *Server* («servidor») *WWW-Authenticate* («autenticar WWW»)

Tabla 22.8. Elementos de HTTP. *(Continuación.)*

MENSAJES DE RESPUESTA	
Códigos de estado de respuesta	
Moved Temporarily («trasladado temporalmente»)	*Request Timeout* («expiración de solicitud»)
See Other («probar otro»)	*Conflict* («conflicto»)
Not Modified («no modificado»)	*Gone* («desaparecido»)
Use Proxy («utilizar representante»)	*Length Required* («longitud requerida»)
Bad Request («solicitud incorrecta»)	*Unless True* («condición verdadera»)
Unauthorized («desautorizado»)	*Internal Server Error* («error interno del servidor»)
Payment Required («pago requerido»)	*No Implemented* («no implementada»)
Forbidden («prohibido»)	*Bad Gateway* («error en pasarela»)
Not Found («no encontrado»)	*Server Unavailable* («servidor no disponible»)
Method Not Allowed («método no admitido»)	*Gateway Timeout* («expiración de pasarela»)
None Acceptable («ninguno aceptable»)	*extension code* («código de extensión»
Proxy Authentication Required («autenticación de representante requerida»)	

Métodos de solicitud

Un mensaje de solicitud completo comienza siempre con una *Request-Line*, que tiene el siguiente formato:

Request-Line = Method SP Request-URL SP HTTP-Version CRLF

El parámetro «Method» contiene la orden real de solicitud, denominada «método» en HTTP. *Request-URL* es la URL del recurso solicitado y HTTP-Version es el número de versión de HTTP utilizado por el emisor.

Se definen los siguientes métodos de solicitud en HTTP/1.1:

- ***OPTIONS* («opciones»):** una solicitud de información acerca de las opciones disponibles para la cadena de solicitud/respuesta identificada por esta URL.
- ***GET* («obtener»):** una solicitud para obtener la información identificada por la URL, devuelta en un cuerpo de entidad. Una operación *GET* es condicional si el campo de cabecera «If-Modified-Since» está incluido y es parcial si el campo de cabecera «Range» está incluido.
- ***HEAD* («cabecera»):** esta petición es idéntica a GET, exceptuando que la respuesta del servidor no debe incluir un cuerpo de entidad. Todos los campos de la cabecera de la respuesta son lo mismos que en el caso de que el cuerpo de la entidad estuviese presente. Esto permite a un cliente obtener información sobre un recurso sin transferir el cuerpo de la entidad.
- ***POST* («enviar»):** es una solicitud para aceptar la entidad adjunta como una nueva subordinada a la URL identificada. La entidad enviada está subordinada a esa URL de la misma manera que un fichero está subordinado al directorio que lo contiene, una noticia está subordinada a un grupo de noticias al cual se envía o un registro está subordinado a una base de datos.
- ***PUT* («poner»):** es una solicitud para aceptar la entidad adjunta y almacenarla bajo la URL proporcionada. Ésta puede ser un nuevo recurso con una nueva URL o la sustitución del contenido de un recurso existente en una URL.

- ***PATCH* («parchear»):** similar a una orden *PUT*, exceptuando que la entidad contiene una lista de diferencias con respecto al contenido del recurso original identificado en la URL.
- ***COPY* («copiar»):** solicita que una copia del recurso identificado por la URL en *Request-Line* se copie en la(s) localización(es) indicada(s) en el campo *URL-Header* de la cabecera *Entity-Header* de este mensaje.
- ***MOVE* («mover»):** solicita que el recurso identificado por la URL en *Request-Line* se transfiera a la(s) localización(es) indicadas(s) en el campo *URL-Header* de *Entity-Header* de este mensaje. Es equivalente a una orden *COPY* seguida por una orden *DELETE*.
- ***DELETE* («eliminar»):** solicita que el servidor origen elimine el recurso identificado por la URL en *Request-Line*.
- ***LINK* («enlazar»):** establece una o más relaciones de enlace entre los recursos identificados en *Request-Line*. Los enlaces se definen en el campo enlace de *Entity-Header*.
- ***UNLINK* («desenlazar»):** deshace una o más relaciones de enlace del recurso identificado en *Request-Line*. Los enlaces se definen en el campo enlace de *Entity-Header*.
- ***TRACE* («trazar»):** solicita que el servidor devuelva todo lo que reciba como cuerpo de la entidad de la respuesta. Este método se puede emplear con fines de comprobación y diagnóstico.
- ***WRAPPED* («empaquetado»):** permite a un cliente enviar una o más solicitudes encapsuladas. Las solicitudes pueden estar cifradas o procesadas de otra manera. El servidor debe desempaquetar las solicitudes y procesarlas adecuadamente.
- ***Extension-method* («método de extensión»):** permite definir métodos adicionales sin modificar el protocolo, aunque no se puede suponer que el receptor los reconozca.

Campos de la cabecera de solicitud

Los campos de la cabecera de solicitud actúan como modificadores de la solicitud, proporcionando información adicional y parámetros relacionados con la petición. En HTTP/1.1 se definen los siguientes campos:

- ***Accept* («aceptar»):** consiste en una lista de tipos de contenidos y rangos que son admisibles como respuesta a esta petición.
- ***Accept-Charset* («aceptar conjunto de caracteres»):** una lista de conjuntos de caracteres admisibles en la respuesta.
- ***Accept-Encoding* («aceptar esquema de codificación»):** lista de los esquemas de codificación de contenido admisibles para el cuerpo de la entidad. Las codificaciones del contenido se utilizan principalmente para permitir la compresión o el cifrado de un documento. Normalmente, el recurso se almacena con esta codificación y sólo se decodifica antes de su uso real.
- ***Accept-Language* («aceptar lenguaje»):** restringe el conjunto de lenguajes naturales que se prefieren para la respuesta.
- ***Authorization* («autorización»):** contiene un valor de campo, conocido como *credencial*, utilizado por el cliente para autenticarse ante el servidor.

- ***From* («de»):** la dirección de correo electrónico en Internet del usuario humano que controla el agente de usuario solicitante.
- ***Host* («computador»):** especifica el computador en Internet del recurso solicitado.
- ***if-Modified-Since* («si ha sido modificado desde»):** utilizado con el método *GET*. Esta cabecera incluye un parámetro de fecha/hora. El recurso se va a transferir sólo si ha sido modificado desde la fecha/hora especificada. Esta característica permite realizar actualizaciones eficientes de la caché. Un mecanismo que implemente una caché puede emitir periódicamente mensajes *GET* a un servidor origen, recibiendo sólo pequeños mensajes de respuesta a menos que sea necesaria una actualización.
- ***Proxy-Authorization* («autorización del representante»):** permite que un cliente se autentique a un representante que requiera autenticación.
- ***Range* («rango»):** para su estudio futuro. Se pretende que, en un mensaje *GET*, un cliente pueda solicitar sólo una parte del recurso identificado.
- ***Referrer* («remitente»):** es la URL del recurso del cual se obtuvo *Request-URL*. Esto permite a un servidor generar una lista de enlaces inversos.
- ***Unless* («a menos que»):** funcionamiento similar al campo *If-Modified-Since*, con dos diferencias: (1) no se restringe al método GET y (2) la comparación se realiza en el valor de cualquier campo de *Entity-Header* en lugar de un valor fecha/hora.
- ***User-Agent* («agente de usuario»):** contiene información acerca del agente de usuario que origina esta solicitud. Se utiliza con propósitos estadísticos, para hacer un seguimiento de las violaciones del protocolo y para el reconocimiento automático de agentes usuario con objeto de confeccionar respuestas que eviten las limitaciones particulares de un agente de usuario.

MENSAJES DE RESPUESTA

Un mensaje de respuesta completo consta de una línea de estado seguida por una o más cabeceras generales, de respuesta y de entidad, seguidas por un cuerpo opcional de entidad.

Códigos de estado

Un mensaje de respuesta completo siempre comienza con una *Status-Line*, que tiene el siguiente formato:

Status-Line = HTTP-Version SP Status-Code SP Reason-Phrase CRLF

El valor de HTTP-Version es el número de versión de HTTP utilizado por el emisor. *Status-Code* es un entero de 3 dígitos que indica la respuesta a una solicitud recibida y *Reason-Phrase* proporciona una breve explicación textual del código de estado.

En HTTP/1.1 se define un gran número de códigos de estado. En la Tabla 22.9 se muestran estos códigos junto a una breve explicación. Los códigos se organizan en las siguientes categorías:

- **Informativo:** la solicitud se ha recibido y el procesamiento continúa. Esta respuesta no se acompaña con un cuerpo de entidad.
- **De éxito:** la solicitud se ha recibido correctamente, ha sido comprendida y aceptada. La información devuelta en el mensaje de respuesta depende del método de la solicitud, como se indica a continuación:

  - GET: el contenido del cuerpo de entidad corresponde al recurso solicitado.
  - HEAD: no se devuelve cuerpo de entidad.
  - SEND: la entidad describe o contiene el resultado de la acción.
  - TRACE: la entidad contiene el mensaje de solicitud.
  - Otros métodos: la entidad describe el resultado de la acción.
- **De redirección:** se requiere llevar a cabo acciones adicionales para completar la solicitud.
- **De error del cliente:** la solicitud contiene un error de sintaxis o la solicitud no se puede realizar.
- **De error del servidor:** el servidor falló al llevar a cabo una solicitud aparentemente válida.

Campos de la cabecera de respuesta

Los campos de la cabecera de respuesta proporcionan información adicional que no se puede indicar en la *Status-Line*. En HTTP/1.1 se definen los siguientes campos:

- ***Location*** **(«Localización»):** indica la localización exacta del recurso identificado por *Request-URL*.
- ***Proxy-Authenticate*** **(«autenticación del representante»):** incluido en la respuesta que tenga un código de estado de *Proxy Authentication Required* («autenticación del representante requerida»). Este campo contiene un «reto» que indica el esquema de autentificación y los parámetros requeridos.
- ***Public*** **(«público»):** enumera los métodos no normalizados que admite este servidor.

Tabla 22.9. Códigos de estado HTTP.

Informativo	
Continue («continuar»)	Recibida la parte inicial de la solicitud; el cliente puede continuar con la solicitud.
Switching Protocols («cambiando de protocolo»)	El servidor conmutará al nuevo protocolo de aplicación solicitado.
De éxito	
OK («correcto»)	La solicitud ha tenido éxito y se incluye la información de respuesta apropiada.
Created («creado»)	La solicitud se ha completado y se ha creado un nuevo recurso. Se incluye/n el/los URI.
Accepted («aceptada»)	La solicitud se ha aceptado pero el procesamiento no ha terminado. Puede, o no, que se complete la solicitud.
Non-Authoritative («información no acreditada»)	Los contenidos devueltos de la cabecera de entidad no son el conjunto definitivo disponible del servidor origen, pero se han obtenido de una copia local o una tercera parte.
No Content («sin contenido»)	El servidor ha completado la solicitud, pero no hay información que devolver.
Reset Content («reiniciar contenido»)	La solicitud ha tenido éxito y el agente de usuario debe inicializar la vista de documento que causó la generación de la solicitud.
Partial Content («contenido parcial»)	El servidor ha completado la solicitud GET parcial y se incluye la información correspondiente.

Tabla 22.9. Códigos de estado HTTP (*continuación*).

De redirección	
Multiples Choices («múltiples alternativas»)	El recurso solicitado está disponible en varias localizaciones y no se puede determinar la localización preferida.
Moved Permanently («trasladado permanentemente»)	Al recurso solicitado se le ha asignado un URI permanente nuevo. Futuras referencias deben hacerse a este URI.
Moved Temporarily («trasladado temporalmente»)	El recurso solicitado reside temporalmente en un URI diferente.
See Other («probar otro»)	La respuesta a la solicitud se puede encontrar en un URI diferente, y debe conseguirse mediante la orden GET sobre ese recurso.
Not Modified («no modificado»)	El cliente ha emitido una orden GET condicional, el acceso está permitido, y el documento no se ha modificado desde la fecha/hora especificada en la solicitud.
Use Proxy («utilizar representante»)	El recurso solicitado se debe acceder a través del representante indicado en el campo *Location*.
De error del cliente	
Bad Fequest («solicitud incorrecta»)	Sintaxis incorrecta en la solicitud.
Unathorized («desautorizado»)	La solicitud requiere la autenticación del usuario.
Payment Required («pago requerido»)	Reservado para usos futuros.
Forbidden («prohibido»)	El servidor rechaza completar la solicitud. Se utiliza cuando el servidor no desea revelar por qué rechazó la solicitud.
Not Found («no encontrado»)	No se encontró el URI solicitado.
Method Not Allowed («método no admitido»)	Método (orden) no permitido para el recurso solicitado.
None Acceptable («ninguno aceptable»)	Se ha encontrado un recurso que corresponde con el URI solicitado, pero que no satisface las condiciones especificadas en la solicitud.
Proxy Authentication Required («autenticación de representante requerida»)	El cliente se debe autenticar primero con el representante.
Request Timeout («expiración de solicitud»)	El cliente no produjo una solicitud dentro del tiempo en que el servidor estaba preparado para esperar.
Conflict («conflicto»)	La solicitud no se pudo llevar a cabo debido a un conflicto con el estado actual del recurso.
Gone («desaparecido»)	El recurso solicitado ya no está disponible en el servidor y no se conoce ninguna dirección de reenvío.
Length Required («longitud requerida»)	El servidor rechaza aceptar solicitudes sin la especificación de la longitud del contenido.
Unless True («condición verdadera»)	La condición dada en el campo *Unless* que era verdadera cuando se comprobó en el servidor.
De error del servidor	
Internal Server Error («error interno servidor»)	El servidor encontró una condición no esperada que le impidió llevar a cabo la solicitud.
Not Implemented («no implementada»)	El servidor no soporta la funcionalidad requerida para llevar a cabo la solicitud.
Bad Gateway («error en pasarela»)	El servidor, mientras actuaba como pasarela o representante, recibió una respuesta no válida del servidor al que accedió para llevar a cabo la solicitud.
Service Unavailable («servidor no disponible»)	El servidor es incapaz de gestionar la solicitud debido a una sobrecarga temporal o a mantenimiento del servidor.
Gateway Timeout («expiración de pasarela»)	El servidor, mientras actuaba como pasarela o representante, no recibió una respuesta a tiempo del servidor al que accedió para llevar a cabo la solicitud.

- ***Retry-After* («intentar después de»):** incluido en la respuesta que tenga un código de estado correspondiente a *Service Unavailable* («servicio no disponible»). Indica cuánto tiempo se espera que el servicio siga sin estar disponible.
- ***Server* («servidor»):** identifica el producto software utilizado por el servidor origen para procesar la solicitud.
- ***WWW-Authenticate* («Autenticar WWW»):** incluida en la respuesta que tenga el código de estado correspondiente a *Unauthorized* («desautorizado»). Este campo contiene un «reto» que indica el esquema de autenticación y los parámetros requeridos.

ENTIDADES

Una entidad consta de una cabecera de entidad y un cuerpo de entidad dentro de un mensaje de solicitud o de respuesta. Una entidad puede representar un recurso de datos o puede constituir otra información proporcionada con una solicitud o una respuesta.

Campos de la cabecera de entidad

Los campos de la cabecera de entidad proporcionan información opcional acerca del cuerpo de la entidad o, si el cuerpo no está presente, sobre el recurso identificado por la solicitud. En HTTP/1.1 se definen los siguientes campos:

- ***Allow* («admitir»):** lista los métodos que el recurso identificado en *Request-URL* admite. Este campo se debe incluir en una respuesta que tenga un código de estado correspondiente a Método No Admitido, y puede incluirse en otras respuestas.
- ***Content-Encoding* («esquema de codificación del contenido»):** indica qué codificaciones de contenido se han aplicado sobre el recurso. La única codificación actualmente definida es la compresión zip.
- ***Content-Language* («lenguaje del contenido»):** identifica el/los lenguaje(s) natural(es) de la audiencia destino de la entidad adjunta.
- ***Content-length* («longitud del contenido»):** especifica el tamaño del cuerpo de la entidad en bytes.
- ***Content-MD5* («MD5 del contenido»):** para su estudio futuro. MD5 se refiere a la función de dispersión segura MD5, descrita en el Capítulo 21.
- ***Content-Range* («rango del contenido»):** para su estudio futuro. Pretende especificar un fragmento del recurso identificado que se incluye en esta respuesta.
- ***Content-Type* («tipo de contenido»):** indica el tipo de contenido del cuerpo de la entidad.
- ***Content-Version* («versión del contenido»):** una etiqueta de versión asociada a una entidad en desarrollo.
- ***Derived-From* («derivada de»):** indica la etiqueta de versión del recurso del cual se derivó esta entidad antes de que el emisor efectuara modificaciones sobre ella. Este campo y el campo Versión del contenido los puede utilizar un grupo de usuarios para gestionar múltiples actualizaciones.
- ***Expires* («expiración»):** fecha/hora después de la cual la entidad se debe considerar obsoleta.

- ***Last-Modified* («última modificación»):** fecha/hora en la que el emisor cree que fue modificado el recurso por última vez.
- ***Link* («enlace»):** define enlaces a otros recursos.
- ***Title* («título»):** un título textual de la entidad.
- ***Transfer-Encoding* («Esquema de codificación de transferencia»):** indica qué tipo de transformación se ha aplicado al cuerpo del mensaje para efectuar una transferencia fiable entre el emisor y el destino. La única codificación definida en el estándar es *fragmentado*. Esta opción define un procedimiento para dividir un cuerpo de entidad en fragmentos etiquetados que se transmiten por separado.
- ***URL-Header* («cabecera de URL»):** informa al destino de otras URL a través de las que se puede identificar el recurso.
- ***Extension-Header* («Cabecera de extensión»):** permite definir campos adicionales sin cambiar el protocolo. Sin embargo, no se puede asumir que estos campos sean reconocibles por el destinatario.

Cuerpo de entidad

Un cuerpo de entidad consta de una secuencia arbitraria de bytes. HTTP está diseñado para ser capaz de transferir cualquier tipo de contenido, incluyendo texto, datos binarios, audio, imágenes y vídeo. Cuando un cuerpo de entidad está presente en un mensaje, la interpretación de los bytes del cuerpo se determina por los campos de la cabecera de entidad *Content-Encoding*, *Content-Type* y *Transfer-Encoding*. Estos definen un modelo de codificación ordenado en tres capas:

$$\text{entity-body} := \text{Transfer-Encoding}(\ \text{Content-Encoding}(\ \text{Content-Type}(\ \text{data}\ )\ )\ )$$

Los datos son el contenido de un recurso identificado por una URL. El campo *Content-Type* determina la forma en la que se interpretan los datos. Se puede aplicar un Esquema de codificación del contenido a los datos y almacenarlos en la URL en lugar de los datos originales. Finalmente, en la transferencia se puede aplicar un esquema de codificación de transferencia para formar el cuerpo de entidad del mensaje.

22.3. GESTIÓN DE RED—SNMP

Las redes y los sistemas de procesamiento distribuido son de una importancia crítica y creciente en negocios, gobierno y otras organizaciones. Dentro de una organización dada, la tendencia es la de evolucionar hacia redes más grandes, más complejas y que den soporte a más aplicaciones y a más usuarios. A medida que estas redes crecen en escala, se evidencian dos hechos:

- La red y sus recursos asociados, así como las aplicaciones distribuidas, se vuelven imprescindibles para la organización.
- Hay más cosas que pueden fallar, inhabilitando la red o una parte de ella o degradando su rendimiento hasta un nivel inaceptable.

Una red fiable y extensa no se puede instalar y gestionar sólo con esfuerzo humano. La complejidad de un sistema tal impone el uso de herramientas automáticas de gestión de la red. La urgencia de la necesidad de esas herramientas se incrementa, así como la dificultad de proporcionarlas, si la red incluye equipos de diferentes fabricantes. En respuesta, se han desarrollado normalizaciones

que comprenden los servicios, los protocolos y la base de la información de gestión para tratar la gestión de red.

Esta sección comienza con una introducción a los conceptos globales de la gestión de red estandarizada. El resto de la sección se dedica a la discusión de SNMP, el estándar de gestión de red más utilizado.

SISTEMAS DE GESTIÓN DE RED

Un sistema de gestión de red es un conjunto de herramientas para monitorizar y controlar la red, de forma integrada en los siguientes sentidos:

- Existe una única interfaz de operador con un potente, pero sencillo para el usuario, conjunto de órdenes para llevar cabo la mayoría de las tareas de gestión de red, si no todas.
- Se requiere una cantidad mínima de equipo adicional. Es decir, la mayor parte del hardware y del software requeridos para la gestión de red se incorpora en el equipo de usuario existente.

Un sistema de gestión de red consiste en la incorporación incremental de hardware y software implementado entre componentes de red existentes. El software que se utiliza para llevar a cabo las tareas de gestión de red reside en los computadores y en los procesadores de comunicaciones (por ejemplo, conmutadores de red y encaminadores). Un sistema de gestión de red está diseñado para que la red entera aparezca como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto y a los atributos específicos de cada elemento y cada enlace conocidos por el sistema. Los elementos activos de la red proporcionan al centro de control de red una realimentación regular de información de estado.

PROTOCOLO SIMPLE DE GESTIÓN DE RED, VERSIÓN 1 (SNMPv1)

SNMP fue desarrollado para su uso como herramienta de gestión de red para redes e interconexiones de redes que operasen sobre TCP/IP. Desde entonces, ha sido ampliado para su uso en todos los tipos de entornos de red. El término *protocolo simple de gestión de red* (*SNMP*, *Simple Network Management Protocol*) se utiliza en realidad para referirse a un conjunto de especificaciones para la gestión de redes que incluye al protocolo en sí mismo, la definición de una base de datos y los conceptos asociados.

Conceptos básicos

El modelo de gestión de red que se utiliza en SNMP incluye los siguientes elementos clave:

- Estación de gestión o gestor.
- Agente.
- Base de datos de información de gestión.
- Protocolo de gestión de red.

La **estación de gestión** es normalmente un dispositivo autónomo, pero puede implementarse en un sistema compartido. En cualquier caso, la estación de gestión sirve como interfaz entre el administrador de red humano y el sistema de gestión de red. La estación de gestión tendrá como mínimo:

- Un conjunto de aplicaciones de gestión para el análisis de los datos, recuperación de fallos, etc.
- Una interfaz a través de la cual el gestor de red puede monitorizar y controlar la red.
- La capacidad de traducir los requisitos del administrador de la red en la monitorización y control reales de los elementos remotos de la red.
- Una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades de la red gestionadas.

Sólo los dos últimos elementos son objeto de la estandarización SNMP.

El otro elemento activo en el sistema de gestión de red es el **agente de gestión**. Las plataformas clave, como computadores, puentes, dispositivos de encaminamiento y concentradores, pueden equiparse con software de agente para que puedan así ser gestionados desde una estación de gestión. El agente responde a las solicitudes de información y de realizar acciones efectuadas desde la estación de gestión y puede proporcionarle a la estación información importante no solicitada de forma asíncrona.

Para gestionar los recursos de la red, cada recurso se representa como un objeto. Un objeto es, esencialmente, una variable de datos que representa un aspecto del agente gestionado. La colección de objetos se conoce como **base de datos de información de gestión** (MIB, *Management Information Base*). La MIB funciona como una colección de puntos de acceso para la estación de gestión en el agente. Estos objetos están normalizados entre los sistemas de una clase particular (por ejemplo, todos los puentes admiten los mismos objetos de gestión). Una estación de gestión lleva a cabo la función de monitorización mediante el acceso a los valores de los objetos MIB. Una estación de gestión puede provocar que se lleve a cabo una acción en un agente o cambiar los parámetros de configuración de un agente mediante la modificación de los valores de variables específicas.

La estación de gestión y los agentes están enlazados por un **protocolo de gestión de red**. El protocolo utilizado para la gestión en redes TCP/IP es el protocolo simple de gestión de red (SNMP). Una versión mejorada de SNMP, conocida como SNMPv2, está destinada a ambos tipos de redes, las basadas en OSI y las basadas en TCP/IP. Cada uno de estos protocolos incluye las siguientes capacidades claves:

- **Obtener:** permite a la estación de gestión obtener los valores de los objetos del agente.
- **Establecer:** permite a la estación de gestión establecer valores de los objetos del agente.
- **Notificar:** permite a un agente enviar a la estación de gestión notificaciones no solicitadas sobre eventos importantes.

En un esquema tradicional de gestión de red centralizado, un computador de la configuración tiene el papel de estación de gestión. Pueden existir una o dos estaciones de gestión adicionales para respaldo. El resto de los dispositivos en la red contienen el software de agente y una MIB, para permitir su monitorización y control por parte de la estación de gestión. Conforme las redes crecen en tamaño y en carga de tráfico, un sistema centralizado como el indicado es impracticable. La estación de gestión soporta demasiada carga y se produce demasiado tráfico, con informes desde cada agente atravesando toda la red hasta llegar a la central. En tales circunstancias, una estrategia descentralizada y distribuida (*véase* Figura 22.6) funciona mejor. En un esquema de gestión de red descentralizado puede haber múltiples estaciones de gestión del nivel más alto, que se podrían denominar servidores de gestión. Cada uno de estos servidores podría gestionar directamente una parte del conjunto total de agentes. Sin embargo, para muchos de los agentes, el servidor de

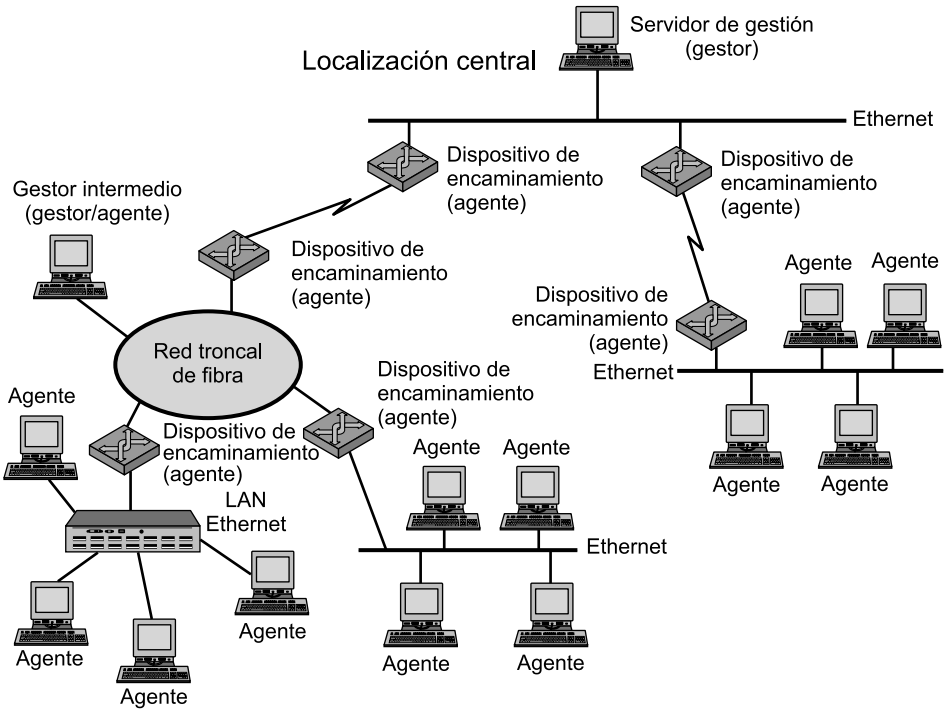


Figura 22.6. Ejemplo de configuración de gestión de red distribuida.

gestión delega la responsabilidad en un gestor intermedio. El gestor intermedio juega el papel de gestor para monitorizar y controlar a los agentes que tiene bajo su responsabilidad. También juega el papel de agente para proporcionar información y aceptar el control de un servidor de gestión de un nivel más alto. Este tipo de arquitectura distribuye la carga de procesamiento y reduce el tráfico total de la red.

Arquitectura del protocolo de gestión de red

SNMP es un protocolo de nivel de aplicación que forma parte del conjunto de protocolos TCP/IP. Se diseñó para operar sobre el protocolo de datagramas de usuario (UDP). La Figura 22.7 propone la configuración típica de los protocolos para SNMPv1. Para una estación de gestión autónoma, un proceso de gestión controla el acceso a una MIB central en la estación de gestión y proporciona una interfaz al gestor de red. El proceso gestor lleva a cabo la gestión de la red mediante el uso de SNMP, implementado sobre UDP, IP y los protocolos dependientes de la red pertinentes (p. ej.: Ethernet, ATM y retransmisión de tramas o *frame relay*).

Cada agente debe implementar también SNMP, UDP e IP. Además, existe un proceso agente que interpreta los mensajes SNMP y controla la MIB del agente. Para un dispositivo agente que dé servicio a otras aplicaciones, como FTP, se requiere que implemente TCP además de UDP. En la Figura 22.7, las partes sombreadas representan el entorno operativo, aquél que va a gestionarse. Las secciones no sombreadas proporcionan soporte a la función de gestión de red.

La Figura 22.8 proporciona una visión un poco más detallada del contexto del protocolo SNMP. Desde una estación de gestión se emiten tres tipos de mensajes SNMP en nombre de una

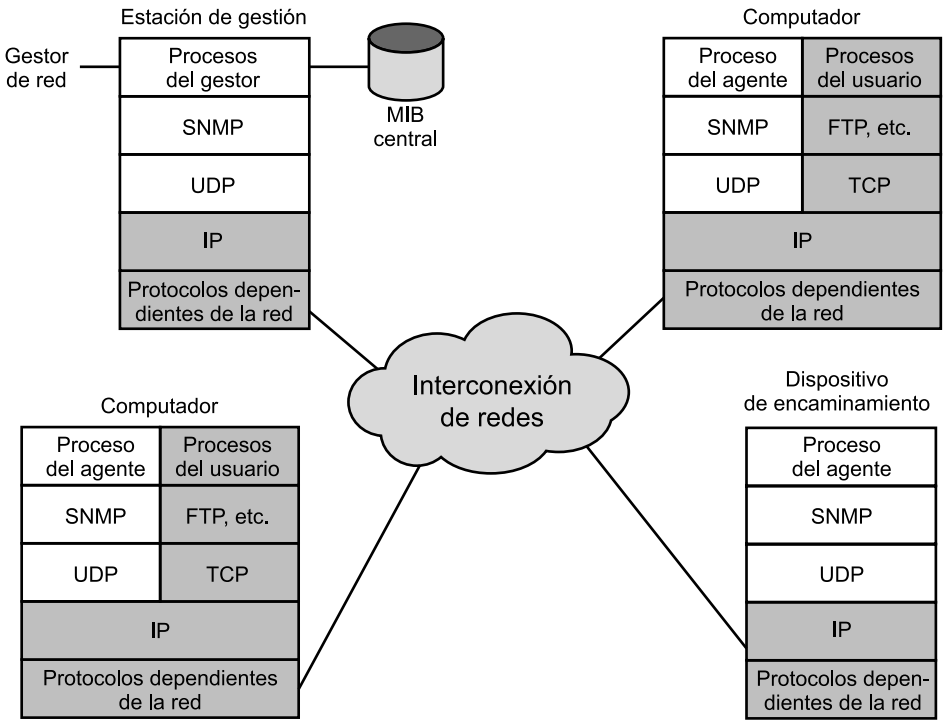


Figura 22.7. Configuración SNMPv1.

aplicación de gestión: *GetRequest* («solicitud obtener»), *GetNextRequest* («solicitud obtener siguiente»), y *SetRequest* («solicitud establecer»). Las dos primeras son variaciones de la función *Get* («obtener»). Los tres mensajes son confirmados por el agente mediante un mensaje *GetResponse*, el cual se pasa a la aplicación de gestión. Además, un agente puede emitir un mensaje de excepción en respuesta a un evento que afecte a la MIB y a los recursos gestionados subyacentes. Las solicitudes de gestión se envían al puerto UDP 161, mientras que el agente envía las excepciones al puerto UDP 162.

Debido a que SNMP utiliza UDP, un protocolo no orientado a conexión, SNMP es en sí mismo no orientado a conexión. No se mantienen conexiones entre una estación de gestión y sus agentes. En su lugar, cada intercambio constituye una transacción diferente entre una estación de gestión y un agente.

PROTOCOLO SIMPLE DE GESTIÓN DE RED, VERSIÓN 2 (SNMPv2)

En agosto de 1988 se publicó la especificación de SNMP y rápidamente se convirtió en el estándar de gestión de red dominante. Diversos fabricantes ofrecen estaciones de trabajo de gestión de red autónomas basadas en SNMP y la mayoría de los fabricantes de puentes, dispositivos de encaminamiento, estaciones de trabajo y PC ofrecen paquetes de agente SNMP que permiten que sus productos sean administrados por una estación de gestión SNMP.

Como su propio nombre indica, SNMP es una herramienta sencilla para la gestión de red. Define una base de datos de información de gestión (MIB) limitada y fácil de implementar, compuesta por variables escalares y tablas de dos dimensiones. Define un protocolo para permitir a un gestor

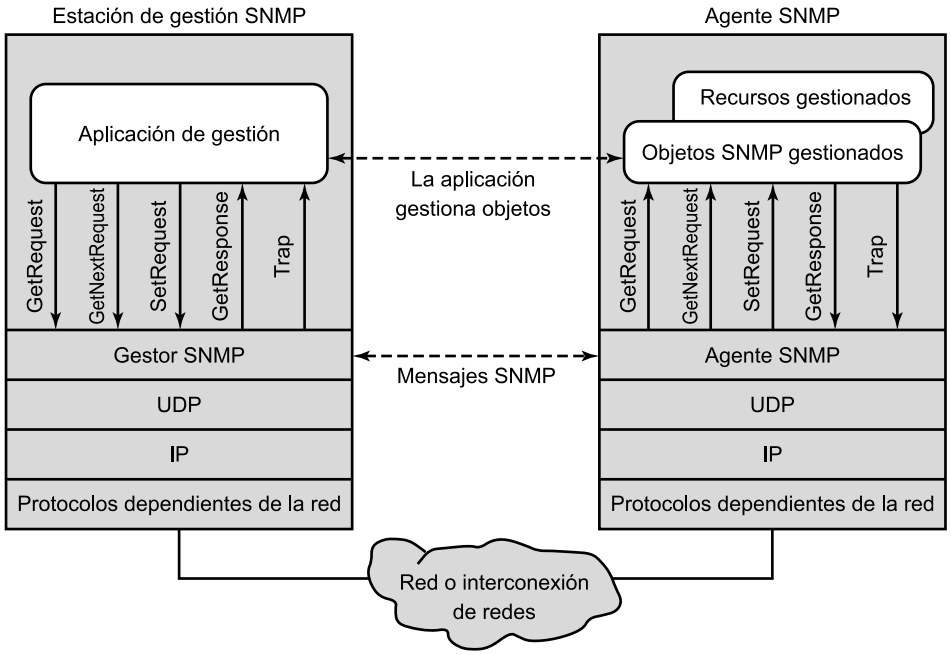


Figura 22.8. El rol de SNMPv1.

obtener y establecer variables MIB y para permitir a un agente emitir notificaciones no solicitadas, denominadas *excepciones* («traps»). La fortaleza de SNMP radica en su simplicidad. SNMP se implementa fácilmente y consume una modesta cantidad de tiempo de procesador y de recursos de red. Además, la estructura del protocolo y de la MIB es suficientemente sencilla, de modo que no es difícil lograr la interoperabilidad entre estaciones de gestión y software de agente de distintos fabricantes.

Con un uso tan extendido, las deficiencias de SNMP se hicieron cada vez más evidentes. Éstas incluyen deficiencias funcionales y la carencia de un servicio de seguridad. Como resultado, se publicó una versión mejorada, conocida como SNMPv2 (RFC 1901, del RFC 1905 al 1909 y del RFC 2578 al RFC 2580). SNMPv2 ganó rápidamente apoyo y varios fabricantes anunciaron productos unos meses después de la publicación del estándar.

Los elementos de SNMPv2

Sorprendentemente, SNMPv2 no proporciona gestión de red en absoluto. En lugar de eso, SNMPv2 proporciona un marco sobre el que se pueden construir aplicaciones de gestión de red. Estas aplicaciones, como gestión de fallos, monitorización del rendimiento, contabilidad, etc., están fuera del ámbito del estándar.

Lo que proporciona SNMPv2 es la infraestructura para la gestión de la red. La Figura 22.9 constituye un ejemplo de configuración que ilustra esa infraestructura.

La base de SNMPv2 es un protocolo que se utiliza para intercambiar información de gestión. Cada participante de un sistema de gestión de red mantiene una base de datos local de información concerniente a la gestión de la red, conocida como la base de datos de información de

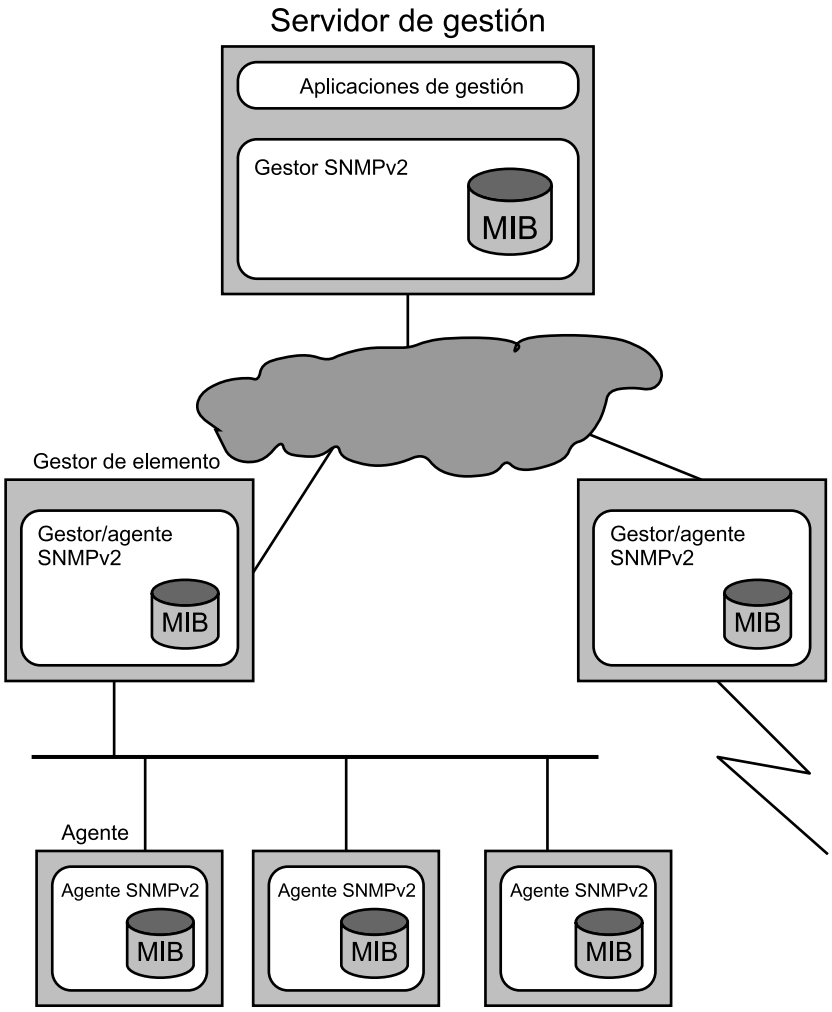


Figura 22.9. Configuración gestionada por SNMPv2.

gestión (MIB). El estándar SNMPv2 define la estructura de esta información y los tipos de datos que admite. A esta definición se le conoce como la estructura de la información de gestión (SMI, *Structure of Management Information*). Podemos verla como el lenguaje para definir la información de gestión. El estándar también proporciona varias MIB que son generalmente útiles para la gestión de red[2]. Además los fabricantes y grupos de usuarios pueden definir nuevas MIB.

Al menos un sistema de la configuración debe ser responsable de la gestión de red. Es ahí donde se hospedan las aplicaciones de gestión de red. Puede haber más de una de estas estaciones de gestión, para proporcionar redundancia o simplemente para repartir responsabilidades en una red amplia. La mayoría del resto de los sistemas actúa como agente. Un agente recoge información

[2] Existe una ligera confusión sobre el término *MIB*. En su forma singular, el término *MIB* se puede utilizar para referirse a toda la base de datos de información en un gestor o en un agente. También se puede utilizar en forma singular o plural para referirse a un conjunto definido concreto de información de gestión que forme parte de una MIB global. Así, el estándar SNMPv2 incluye la definición de varias MIB e incorpora, por referencia, MIB definidas en SNMPv1.

localmente y la almacena para su acceso posterior por parte de un gestor. La información incluye datos sobre el sistema mismo y también puede incluir información del tráfico de la red o redes a las que está conectado el agente.

SNMPv2 dará soporte tanto a una estrategia de gestión de red altamente centralizada como a una estrategia distribuida. En este último caso, algunos sistemas operan como gestor y como agente. En su papel de agente, el sistema aceptará órdenes de un sistema de gestión superior. Algunas de estas órdenes están relacionadas con la MIB local en el agente. Otras órdenes requieren que el agente actúe como representante para dispositivos remotos. En este caso, el agente representante asume el papel de gestor para acceder a información de un agente remoto y después asume el papel de agente para pasar esa información a un gestor superior.

Todos estos intercambios tienen lugar utilizando el protocolo SNMPv2, que es un protocolo sencillo del tipo solicitud/respuesta. Normalmente, se implementa sobre el protocolo de datagrama de usuario (UDP), que es parte de la familia de protocolos TCP/IP. Ya que los intercambios SNMPv2 consisten en pares de solicitud/respuesta discretos, no se requiere una conexión fiable.

Estructura de la información de gestión

La estructura de la información de gestión (SMI) define el marco general dentro del cual se puede definir y construir una MIB. La SMI identifica los tipos de datos que pueden utilizarse en la MIB y cómo se representan y nombran los recursos dentro de la MIB. La filosofía que subyace en la SMI es la de impulsar la simplicidad y la extensibilidad dentro de la MIB. Así, la MIB puede almacenar solamente tipos de datos simples: escalares y matrices de escalares de dos dimensiones llamadas tablas. La SMI no permite la creación o la obtención de estructuras de datos complejas. Esta filosofía contrasta con la utilizada en la gestión de sistemas OSI, que proporciona estructuras de datos y modos de acceso complejos para permitir una mayor funcionalidad. SMI evita los tipos y estructuras de datos complejos para simplificar la tarea de implementación y mejorar su interoperabilidad. Las MIB, inevitablemente, contendrán tipos de datos creados por el fabricante y, a menos que se impongan fuertes restricciones en la definición de tales tipos de datos, la interoperabilidad se verá afectada.

Existen tres elementos clave en la especificación de la SMI. En el nivel más bajo, la SMI especifica los tipos de datos que se pueden almacenar. Después, la SMI especifica una técnica formal para definir los objetos y las tablas de objetos. Finalmente, la SMI proporciona un esquema para asociar un identificador único a cada objeto real de un sistema, con objeto de que un gestor pueda referenciar dichos datos en un agente.

La Tabla 22.10 muestra los tipos de datos que permite la SMI. Éste es un conjunto de tipos bastante restringido. Por ejemplo, no se admiten los números reales. Sin embargo, es lo bastante rico como para satisfacer la mayoría de los requisitos de la gestión de red.

Funcionamiento del protocolo

El núcleo del marco de trabajo de SNMPv2 es el protocolo mismo. Éste proporciona un mecanismo básico y directo para intercambiar información de gestión entre gestor y agente.

La unidad básica de intercambio es el mensaje, que consta de un encapsulado externo del mensaje y de una unidad de datos del protocolo (PDU) interna. La cabecera externa del mensaje se ocupa de la seguridad y será examinada posteriormente en esta sección.

Tabla 22.10. Tipos de datos admisibles en SNMPv2.

Tipo de dato	Descripción
INTEGER	Enteros en el rango de -2^{31} a $2^{31} - 1$.
UInteger32	Enteros en el rango de 0 a $2^{32} - 1$.
Counter32	Un entero no negativo que se puede incrementar módulo 2^{32}.
Counter64	Un entero no negativo que se puede incrementar módulo 2^{64}.
Gauge32	Un entero no negativo que se puede incrementar o disminuir, pero que no excederá de un valor máximo. El valor máximo no puede ser mayor que $2^{32} - 1$.
TimeTicks	Un entero no negativo que representa el tiempo, módulo 2^{32}, en centésimas de segundo.
OCTET STRING	Cadena de octetos para datos arbitrarios binarios o de texto. Puede estar limitado a 255 octetos.
IpAddress	Una dirección de red de 32 bits.
Opaque	Un campo de bits arbitrarios.
BIT STRING	Una enumeración de bits identificados.
OBJECT IDENTIFIER	Nombre asignado administrativamente a objetos u otros elementos normalizados. Su valor es una secuencia de hasta 128 enteros no negativos.

Un mensaje SNMP puede transportar siete tipos de PDU. El formato general de estos tipos se muestra informalmente en la Figura 22.10. Existen varios campos que son comunes a varios tipos de PDU. El campo «identificador de solicitud» es un entero que se asigna de forma que las solicitudes pendientes se puedan identificar de forma unívoca. Esto permite a un gestor correlacionar las respuestas que recibe con las solicitudes pendientes. También permite a un agente hacer frente al problema de las PDU replicadas, generadas por un servicio de transporte no fiable. El campo de «vinculaciones de variables» contiene una lista de identificadores de objeto. Dependiendo de la PDU, la lista puede incluir además un valor para cada objeto.

La PDU *GetRequest*, emitida por un gestor, incluye una lista de uno o más nombres de objetos para los que se solicita su valor. Si la operación de obtención tiene éxito, el agente que responde

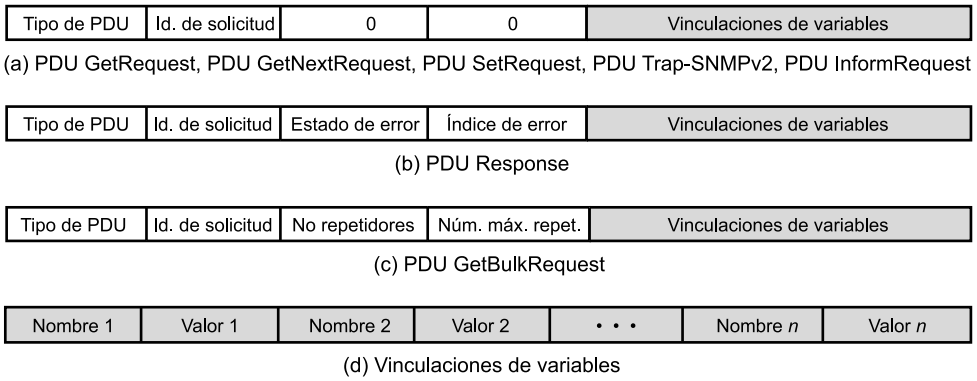


Figura 22.10. Formato de la PDU de SNMPv2.

enviará una PDU *Response* («Respuesta»). La lista de las vinculaciones de variables contendrá el identificador y el valor de todos los objetos obtenidos. Para cualquier variable que no esté en la vista de la MIB pertinente, se devuelve el identificador y un código de error en la lista de vinculaciones de variables. De este modo, SNMPv2 permite respuestas parciales a un *GetRequest*, lo que supone una mejora significativa con respecto a SNMP. En SNMP, si una o más de las variables de un *GetRequest* no se admiten, el agente devuelve un mensaje de error con el estado *noSuchName* («no existe ese nombre»). Para hacer frente a este tipo de error, el gestor SNMP no debe devolver ningún valor a la aplicación solicitante o debe incluir un algoritmo que responda ante un error eliminando las variables perdidas, reenviando la solicitud y enviando un resultado parcial a la aplicación.

La PDU *GetNextRequest* también la emite un gestor e incluye una lista de uno o más objetos. En este caso, para cada uno de los objetos cuyos nombres se encuentren en el campo de vinculaciones de variables se devuelve un valor para el objeto que le siga en orden lexicográfico, lo que es equivalente a decir el siguiente en la MIB en términos de su posición en la estructura de árbol de identificadores de objetos. Como con la PDU *GetRequest*, el agente devolverá los valores de tantas variables como le sea posible. Uno de los puntos fuertes de la PDU *GetNextRequest* consiste en que permite a una entidad gestora descubrir dinámicamente la estructura de una vista de MIB. Esto es útil si el gestor no conoce a priori el conjunto de objetos que proporciona un agente o que existen en una vista de MIB en particular.

Una de las principales mejoras proporcionadas por SNMPv2 es la PDU *GetBulkRequest* («solicitud obtener en lote»). El objetivo de esta PDU es minimizar el número de intercambios del protocolo requeridos para obtener gran cantidad de información de gestión. La PDU *GetBulkRequest* permite a un gestor SNMPv2 solicitar que la respuesta sea tan grande como sea posible, dadas las restricciones del tamaño del mensaje.

La PDU *SetRequest* la emite un gestor para solicitar que se modifique el valor de uno o más objetos. La entidad SNMPv2 que la recibe responde con una PDU *Response* que contiene el mismo «identificador de solicitud». La operación *SetRequest* es atómica: o se actualizan todas las variables o no se actualiza ninguna. Si la entidad que responde es capaz de establecer los valores de todas las variables indicadas en la lista recibida de «vinculaciones de variables», entonces la PDU *Response* incluye el campo de «vinculaciones de variables» proporcionando un valor para cada variable. Si no puede proporcionarse el valor de alguna de las variables, entonces no se devuelve ni actualiza ningún valor. En este último caso, el código de «estado de error» indica la razón del fallo y el campo «índice de error» señala la variable de la lista de «vinculaciones de variables» que causó el fallo.

La PDU *Trap-SNMPv*2 («excepción SNMPv2») la genera y transmite un agente SNMPv2 actuando como agente cuando se produce un evento inusual. Se utiliza para proporcionar a la estación de gestión una notificación asíncrona sobre algún evento significativo. La lista de vinculaciones de variables se utiliza para contener la información asociada con el mensaje de excepción. A diferencia de *GetRequest*, *GetNextRequest*, *GetBulkRequest*, *SetRequest y InformRequest* («solicitud de informe»), la PDU *Trap-SNMPv2* no obtiene una respuesta de la entidad que lo recibe: es un mensaje que no espera confirmación.

La PDU *InformRequest* la envía una entidad SNMPv2 en el papel de gestor en representación de una aplicación a otra entidad SNMPv2 que actúe como gestor, para proporcionar información de gestión a una aplicación que use los servicios de la segunda entidad. Como con la PDU *Trap-SNMPv2*, la lista de vinculaciones de variables se utiliza para transportar la información asociada. El gestor que recibe un *InformRequest* confirma este mensaje con una PDU Response.

Tanto para *Trap-SNMPv2* como para *InformRequest*, se pueden definir varias condiciones que indican cuándo se genera la notificación. También se especifica la información que se ha de enviar.

PROTOCOLO SIMPLE DE GESTIÓN DE RED, VERSIÓN 3 (SNMPv3)

Muchas de las deficiencias funcionales de SNMP se abordaron en SNMPv2. Para corregir las deficiencias en seguridad de SNMPv1 y SNMPv2, se publicó en enero de 1998 SNMPv3 como un conjunto de estándares propuestos (actualmente del RFC 2570 al RFC 2575). Este conjunto de documentos no proporciona un funcionamiento SNMP completo, sino que define una arquitectura general de SNMP y un conjunto de competencias en seguridad. Éstas están pensadas para utilizarse con el SNMPv2 actual.

SNMPv3 proporciona tres servicios importantes: autenticación, privacidad y control de acceso. Los dos primeros forman parte del modelo de seguridad basada en el usuario (USM, *User-Based Security*) y el último se define en el modelo de control de acceso basado en vistas (VACM, *View-Based Access Control Model*). Los servicios de seguridad se guían por la identidad del usuario que solicita el servicio. Esta identidad se conoce como «director», que puede ser un individuo, una aplicación o un grupo de individuos o de aplicaciones.

El mecanismo de autenticación en USM asegura que el mensaje recibido lo transmitió el director cuya identidad aparece como origen en la cabecera del mensaje. Este mecanismo también asegura que el mensaje no ha sido modificado durante su transmisión y que no ha sido retardado o retransmitido artificialmente. El director emisor proporciona la autenticación mediante la inclusión de un código de autenticación del mensaje en el mensaje SNMP que está enviando. Este código es una función del contenido del mensaje, de las identidades de las partes emisora y receptora, del instante de la transmisión y de una clave secreta que deben conocer sólo el emisor y el receptor. La clave secreta se debe establecer fuera de USM como una función de configuración. Es decir, el gestor de configuración o el gestor de red es el responsable de la distribución de las claves secretas que se han de cargar en las bases de datos de los diferentes gestores y agentes SNMP. Esto se puede llevar a cabo manualmente o utilizando alguna forma de transferencia segura de datos fuera de USM. Cuando el director receptor obtiene el mensaje, utiliza la misma clave secreta para calcular el código de autenticación del mensaje de nuevo. Si la versión del código en el receptor coincide con el valor incorporado al mensaje recibido, entonces el receptor sabe que el mensaje sólo lo puede haber originado el gestor autorizado y que el mensaje no fue alterado en el camino. La clave secreta compartida por el emisor y el receptor debe ser configurada con antelación. El código de autenticación real utilizado se conoce como HMAC, que es un mecanismo de autenticación estándar de Internet.

El servicio de privacidad de USM permite cifrar mensajes a los gestores y a los agentes. De nuevo, el gestor director y el agente director deben compartir una clave secreta. En este caso, si los dos se configuran para hacer uso del servicio de privacidad, todo el tráfico entre ellos se cifra empleando el estándar de cifrado de datos (DES). El director emisor cifra el mensaje utilizando el algoritmo DES y su clave secreta y envía el mensaje al director receptor, quien lo descifra mediante el algoritmo DES y la misma clave secreta.

El servicio de control de acceso hace posible configurar los agentes para que proporcionen a distintos gestores diferentes niveles de acceso a la base de datos de información de gestión (MIB) del agente. Un director agente puede restringir a un director gestor el acceso a su MIB de dos formas. En primer lugar, puede restringir el acceso a cierta sección de su MIB. Por ejemplo, un agente podría restringir a la mayoría de los gestores ver las estadísticas relativas al rendimiento y permitir ver y actualizar los parámetros de configuración solamente a un único director gestor designado para ello. En segundo lugar, el agente puede limitar las operaciones que un gestor puede utilizar sobre esa sección de la MIB. Por ejemplo, se podría limitar a un director gestor determinado a un acceso de sólo lectura sobre una sección de la MIB de un agente. La política de control de

acceso que ha de utilizar un agente para cada gestor se debe configurar previamente y, esencialmente, consiste en una tabla que detalla los privilegios de acceso de los diferentes gestores autorizados.

22.4. LECTURAS Y SITIOS WEB RECOMENDADOS

[ROSE98] proporciona un extenso tratamiento sobre el correo electrónico, incluyendo algún estudio sobre SMTP y MIME. [KRIS01] proporciona un buen estudio sobre HTTP. [STAL99] presenta un riguroso y detallado examen de SNMP, SNMPv2 y SNMPv3. Este libro proporciona además una descripción general de la tecnología de gestión de redes.

KRIS01 Krishnamurthy, B., y Rexford, J. *Web Protocols and Practice: HTTP/1.1, Networking Protocols, Caching, and Traffic Measurement.* Upper Saddle River, NJ: Prentice Hall, 2001

ROSE98 Rose, M., y Strom, D. *Internet Messaging*: *From the Desktop to the Enterprise*. Upper Saddle River, NJ: Prentice Hall, 1998.

STAL99 Stallings, W. *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*. Reading, MA: Addison-Wesley, 1999.

SITIOS WEB RECOMENDADOS

- **Consorcio WWW:** contiene información actualizada sobre HTTP y temas relacionados.
- **Página web «Simple»:** mantenida por la Universidad de Twente, constituye una buena fuente de información sobre SNMP, incluyendo enlaces a muchas implementaciones de dominio público y listas de libros y artículos.

22.5. TÉRMINOS CLAVE, CUESTIONES DE REPASO Y PROBLEMAS

TÉRMINOS CLAVE

agente
base-64
base de datos de información de gestión (MIB)
codificación radix-64
correo electrónico
estación de gestión
extensiones multipropósito de correo electrónico (MIME)
protocolo de transferencia de hipertexto (HTTP)
protocolo de gestión de red
protocolo simple de gestión de red (SNMP)
protocolo simple de transferencia de correo (SMTP)
representante
sistema de gestión de red

CUESTIONES DE REPASO

22.1. ¿Cuál es la diferencia entre el RFC 821 y el RFC 822?

22.2. ¿Qué son los estándares SMTP y MIME?

22.3. ¿Cuál es la diferencia entre un tipo de contenido MIME y un esquema de codificación de transferencia MIME?

22.4. Explique brevemente la codificación radix-64.

22.5. Explique las diferencias entre representante, pasarela y túnel HTTP.

22.6. ¿Qué es un sistema de gestión de red?

22.7. Enumere y defina brevemente los elementos clave de SNMP.

22.8. ¿Qué funciones proporciona SNMP?

22.9. ¿Cuáles son las diferencias entre SNMPv1, SNMPv2 y SNMPv3?

EJERCICIOS

22.1. Los sistemas de correo electrónico difieren en la manera en la que se procesan múltiples destinatarios. En algunos sistemas, el agente de usuario origen o el emisor de correo realiza todas las copias necesarias y las envía de forma independiente. Una alternativa a esto consiste en determinar primero la ruta a cada destino y enviar después un único mensaje por la parte común de las rutas, realizando copias solamente cuando las rutas divergen. Este proceso se conoce como empaquetado de correo (*mail-bagging*). Discuta las ventajas y desventajas de los dos métodos.

22.2. La especificación original (versión 1) de SNMP establece la siguiente definición para un nuevo tipo de datos:

Indicador :: = [APLICACIÓN 2] IMPLICIT INTEGER (0..4294967295)

El estándar incluye la siguiente explicación sobre la semántica de este tipo:

> Este tipo de datos de aplicación representa un entero no negativo que puede incrementarse o disminuir, pero que conmuta al llegar a un valor máximo. Este estándar especifica un valor máximo de $2^{23} - 1$ (4294967295 en decimal) para el tipo Indicador.

Desafortunadamente, la palabra «conmutar» no está definida en la especificación y ha dado lugar a dos interpretaciones diferentes. El estándar SNMPv2 clarifica esta ambigüedad con la siguiente definición:

> El valor de indicador es máximo siempre que la información que se modela es mayor o igual que ese valor máximo. Si la información que se está modelando disminuye posteriormente por debajo del valor máximo, el indicador también disminuye.

a) ¿Cuál es la interpretación alternativa?

b) Discuta las ventajas e inconvenientes de las dos interpretaciones.

22.3. Excluyendo el establecimiento de conexión y cierre, ¿cuál es el mínimo número de rondas de ida y vuelta en la red necesarias para enviar un mensaje corto de correo utilizando SMTP?

22.4. Aunque TCP es un protocolo *full-duplex*, SMTP utiliza TCP en modo *half-duplex*: el cliente envía una orden y entonces se detiene para esperar la respuesta. ¿Cómo puede este funcionamiento *half-duplex* confundir al mecanismo de arranque lento de TCP cuando la red está al límite de su capacidad?

22.5. Debido a que SNMP utiliza dos números de puertos diferentes (puertos UDP 161 y 162), un solo sistema puede fácilmente ejecutar un gestor y un agente. ¿Qué ocurriría si el mismo número de puerto se utilizara para ambos?

APÉNDICE A

RFC citados en este libro

Número	Título	Fecha
768	Protocolo de datagrama de usuario (UDP).	1980
791	Protocolo Internet (IP).	1981
792	Protocolo de mensajes de control de Internet (ICMP).	1981
793	Protocolo de control de transmisión (TCP).	1981
821	Protocolo simple de transferencia de correo (SMTP).	1982
822	Normalización para el formato de mensajes de texto de Internet de ARPA.	1982
959	Protocolo de transferencia de ficheros (FTP).	1985
1350	Protocolo trivial de transferencia de ficheros (Revisión 2).	1992
1633	Servicios integrados en la arquitectura de Internet: una visión general.	1994
1636	Seguridad en la arquitectura de Internet.	1994
1752	Recomendación para el protocolo IP de próxima generación.	1995
1771	Protocolo 4 de pasarela frontera (BGP-4).	1995
1812	Requisitos para los encaminadores IP versión 4.	1995
1901	Introducción a SNMPv2 basado en comunidad.	1996
1905	Operaciones de protocolo de SNMPv2.	1996
1906	Alternativas para el transporte de SNMPv2.	1996
1907	Base de datos de información de gestión para SNMPv2.	1996
1908	Coexistencia entre la versión 1 y la versión 2 de la normalización de gestión de red para Internet.	1996
1909	Infraestructura administrativa para SNMPv2.	1996
2045	Extensiones multipropósito de correo electrónico (MIME), primera parte: formato del cuerpo de mensaje en Internet.	1996
2046	Extensiones multipropósito de correo electrónico (MIME) segunda parte: tipos de información.	1996
2047	MIME (Extensiones multipropósito de correo electrónico), tercera parte: extensiones de la cabecera del mensaje para texto no ASCII.	1996
2048	Extensiones multipropósito de correo electrónico (MIME), cuarta parte: procedimientos de registro.	1996
2049	Extensiones multipropósito de correo electrónico (MIME), quinta parte: criterios de conformidad y ejemplos.	1996
2205	Especificación funcional del protocolo de reserva de recursos (RSVP)-Versión 1.	1997
2246	El protocolo TLS.	1999
2328	Protocolo del primer camino más corto disponible (OSPF), versión 2.	1998
2373	Arquitectura de direccionamiento IP, versión 6.	1998

Número	Título	Fecha
2401	Arquitectura de seguridad para el protocolo de Internet.	1998
2402	Cabecera de autentificación de IP.	1998
2406	Encapsulado de la carga útil de seguridad (ESP) de IP.	1998
2408	Asociación de seguridad en Internet y protocolo de gestión de claves.	1998
2460	Especificación del protocolo Internet versión 6.	1998
2474	Definición del campo de servicios diferenciados en las cabeceras de IPv4 e IPv6.	1998
2475	Arquitectura para servicios diferenciados.	1998
2570	Introducción a la versión 3 de la normalización de gestión de red para Internet.	1999
2571	Arquitectura para la descripción de entornos de gestión SNMP.	1999
2572	Procesamiento y gestión de mensajes SNMP.	1999
2573	Aplicaciones SNMP.	1999
2574	Modelo de seguridad basado en usuario para SNMPv3.	1999
2575	Modelo de control de acceso basado en vistas (VACM) para SNMP.	1999
2578	Estructura de información de gestión, versión 2 (SMIv2).	1999
2579	Convenciones textuales para SMIv2.	1999
2580	Declaraciones de conformidad para SMIv2.	1999
2597	Grupo de PHB de reenvío asegurado.	1999
2581	Control de congestión TCP.	1999
2616	Protocolo de transferencia de hipertexto-HTTP/1.1.	1999
2828	Glosario de seguridad en Internet.	2000
3015	Protocolo de control de pasarelas multimedia.	2000
3168	Adición de la notificación explícita de congestión (ECN) en IP.	2001
3246	Un comportamiento por salto (PHB) de reenvío urgente.	2002
3376	Protocolo de gestión de grupos en Internet, versión 3.	2002

APÉNDICE B

Análisis de Fourier

En este apéndice se presenta un resumen de los conceptos fundamentales del análisis de Fourier.

B.1. DESARROLLO EN SERIE DE FOURIER PARA SEÑALES PERIÓDICAS

La determinación del contenido en frecuencias de muchas señales se puede obtener fácilmente disponiendo de unas buenas tablas de integrales. Empecemos considerando las señales periódicas. Cualquier señal periódica se puede expresar como una suma de funciones sinusoidales, denominada serie de Fourier[1]:

$$x(t) = \frac{A_0}{2} + \sum_{n=1}^{\infty} [A_n \cos(2\pi n f_0 t) + B_n \operatorname{sen}(2\pi n f_0 t)]$$

donde f_0 es la inversa del periodo de la señal ($f_0 = 1/T$). La frecuencia f_0 se denomina **frecuencia** o **armónico fundamental** y a los múltiplos de f_0 se les conoce como **armónicos**. Por tanto, una señal periódica con periodo T estará compuesta por la frecuencia fundamental $f_0 = 1/T$, más múltiplos enteros de dicha frecuencia. Si A_0 es distinto de 0, la señal $x(t)$ tiene una **componente continua** o **dc**.

Los valores de los coeficientes del desarrollo en serie de Fourier se calculan mediante las siguientes expresiones:

$$A_0 = \frac{2}{T} \int_0^T x(t)\, dt$$

$$A_n = \frac{2}{T} \int_0^T x(t) \cos(2\pi n f_0 t)\, dt$$

$$B_n = \frac{2}{T} \int_0^T x(t) \operatorname{sen}(2\pi n f_0 t)\, dt$$

[1] Los matemáticos generalmente expresan las series y la transformada de Fourier utilizando la variable w_0, con dimensiones de radianes por segundo, siendo $w_0 = 2\pi f_0$. Sin embargo, los físicos e ingenieros prefieren expresarlas en términos de f_0, ya que se simplifican las expresiones, además de que es más intuitivo tener la frecuencia expresada en hertzios en lugar de radianes por segundo.

Este tipo de representación, conocida como representación seno-coseno, es la más sencilla de calcular, si bien presenta el problema de tener dos componentes para cada frecuencia. Otra representación más significativa, denominada representación amplitud-fase, adopta la siguiente forma:

$$x(t) = \frac{C_0}{2} + \sum_{n=1}^{\infty} C_n \cos(2\pi n f_0 t + \theta_n)$$

que se relaciona con la representación seno-coseno mediante las expresiones siguientes:

$$C_0 = A_0$$

$$C_n = \sqrt{A_n^2 + B_n^2}$$

$$\theta_n = \tan^{-1}\left(\frac{-B_n}{A_n}\right)$$

En la Figura B.1 se muestran ejemplos del desarrollo en serie de Fourier para algunas señales periódicas.

B.2. TRANSFORMADA DE FOURIER PARA SEÑALES NO PERIÓDICAS

El espectro de una señal periódica consiste en un conjunto de componentes en frecuencias discretas a la frecuencia fundamental y sus armónicos. Para una señal no periódica, el espectro consiste en un continuo de frecuencias. Este espectro se puede obtener mediante la transformada de Fourier. Para una señal $x(t)$, con espectro $X(f)$, se verifican las siguientes expresiones:

$$x(t) = \int_{-\infty}^{\infty} X(f) e^{j2\pi ft}\, df$$

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft}\, dt$$

donde $j = \sqrt{-1}$. La aparición del número imaginario en las expresiones anteriores es por razones de comodidad. La componente imaginaria tiene una interpretación física relacionada con la fase de la forma de onda, la explicación de esta interpretación está fuera de los objetivos de este libro.

En la Figura B.2 se representan algunas señales junto con sus correspondientes transformadas.

DENSIDAD DE POTENCIA ESPECTRAL Y ANCHO DE BANDA

Estrictamente hablando, el ancho de banda de cualquier señal limitada en el tiempo es infinito. No obstante, en la práctica, la mayor parte de la potencia de la señal se concentra en una banda finita y, en ese caso, el ancho de banda efectivo consiste en la porción del espectro que contiene la mayor parte de la potencia. Para una definición más precisa es necesario introducir el concepto de densidad de potencia espectral (PSD, *Power Spectral Density*). Esencialmente, la PSD describe el contenido en potencias de una señal como función de la frecuencia, de forma que representa cuánta potencia hay en las distintas bandas de frecuencia.

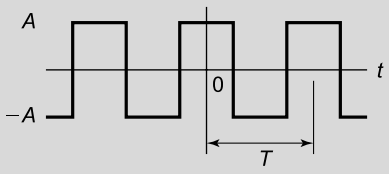
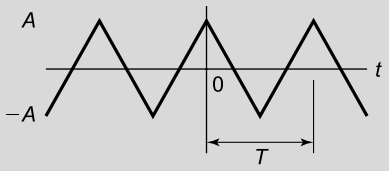
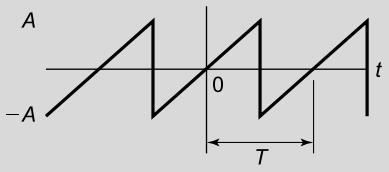
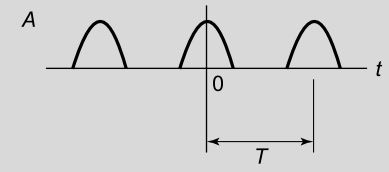
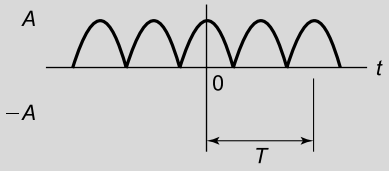
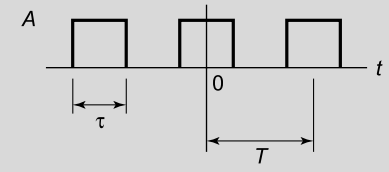
Señal	Desarrollo de las series de Fourier
Onda cuadrada 	$(4A/\pi) \times [\cos(2\pi f_1 t) - (1/3)\cos(2\pi(3f_1)t) + (1/5)\cos(2\pi(5f_1)t) - (1/7)\cos(2\pi(7f_1)t) + \ldots]$
Onda triangular 	$C_0 = 0$ $C_n = 0$ para n par $C_n = 8A/(n\pi)^2$ para n impar
Onda de diente de sierra 	$A_0 = 0$ $A_n = 0$ para n par $B_n = -(-1)^{(n)} \times (2A/\pi n)$
Media onda coseno rectificada 	$C_0 = 2A/\pi$ $C_n = 0$ para n impar $C_n = (2A/\pi) \times (-1)^{(1+n/2)} \times (2/(n^2 - 1))$ para n par
Onda completa coseno rectificada 	$C_0 = 4A/\pi$ $C_n = (4A/\pi) \times (-1)^n \times (1/(4n^2 - 1))$
Tren de pulsos 	$C_n = (2A\tau/T) \times (\text{sen}(n\pi\tau/T)/(n\pi\tau/T))$

Figura B.1. Algunas señales periódicas habituales y su serie de Fourier.

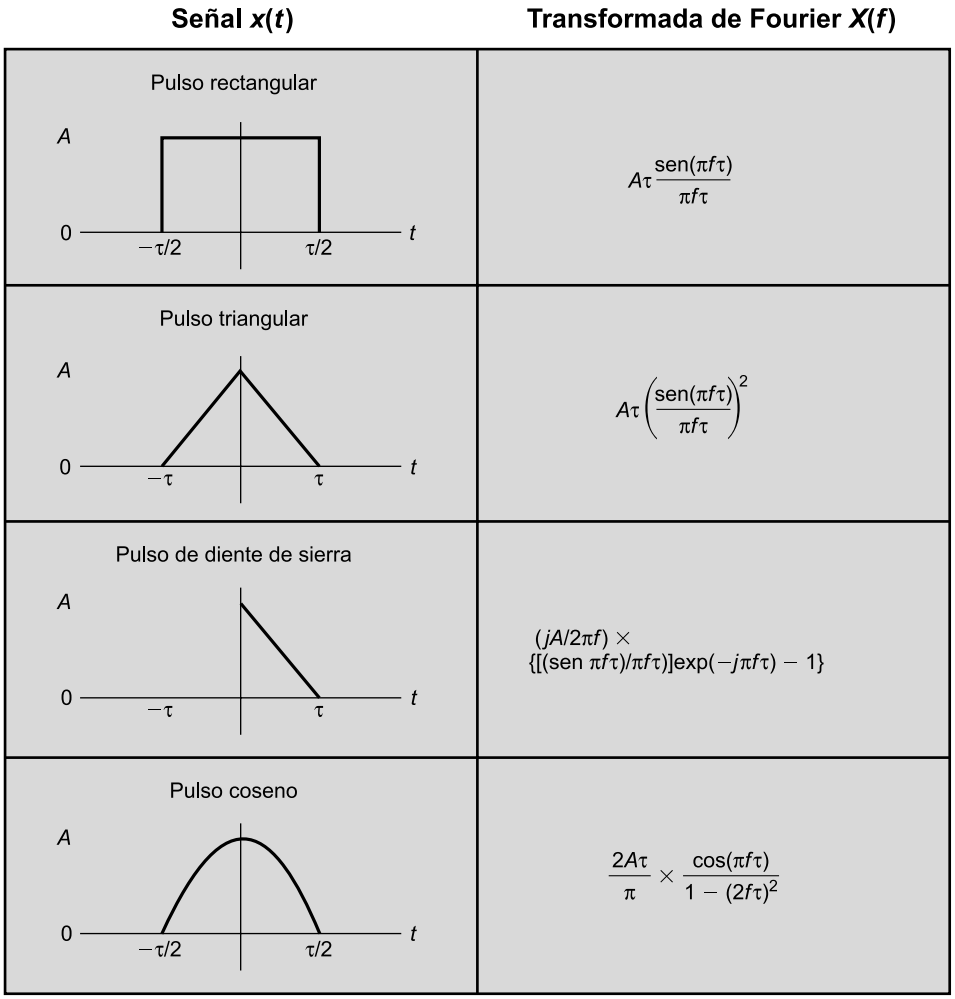


Figura B.2. Algunas señales no periódicas habituales y sus transformadas de Fourier.

Para comenzar, considérese la potencia de la señal en el dominio del tiempo. La función $x(t)$ alude normalmente a una señal en términos de tensión o intensidad. En cualquier caso, la potencia instantánea de la señal es proporcional a $|x(t)|^2$. Para una señal limitada en el tiempo se define la potencia media como

$$P = \frac{1}{t_1 - t_2}\int_{t_1}^{t_2} |x(t)|^2\,dt$$

Para el caso de una señal periódica, la potencia media en un periodo viene dada por

$$P = \frac{1}{T}\int_0^T |x(t)|^2\,dt$$

Sería deseable conocer la distribución de la potencia en función de la frecuencia. Esto se puede hacer fácilmente en términos de los coeficientes del desarrollo en serie de Fourier en el caso de señales periódicas. En ese caso, la densidad de potencia espectral $S(f)$ es

$$S(f) = \sum_{n=-\infty}^{\infty} |C_n|^2 \delta(f - nf_0)$$

donde f_0 es la inversa del periodo de la señal ($f_0 = 1/T$), C_n es el coeficiente de las series de Fourier en su representación amplitud-fase y $\delta(t)$ es el impulso unitario o función delta, definido por:

$$\delta(t) = \begin{cases} 0 & \text{si} \quad t \neq 0 \\ \infty & \text{si} \quad t = 0 \end{cases}$$

$$\int_{-\infty}^{\infty} \delta(t)\, dt = 1$$

La densidad de potencia espectral $S(f)$ para una señal no periódica es más difícil de definir. Básicamente, se obtiene definiendo un «periodo» T_0 y permitiendo que T_0 aumente sin límite.

Para una función continua $S(f)$, la potencia contenida en la banda de frecuencias definida por $f_1 < f < f_2$, viene dada por

$$P = 2 \int_{f_1}^{f_2} S(f)\, df$$

Si la forma de onda es periódica, la potencia contenida en los j primeros armónicos es

$$P = \frac{1}{4} C_0^2 + \frac{1}{2} \sum_{n=1}^{j} C_n^2$$

Habiendo definido los conceptos anteriores, se está en disposición de definir el denominado ancho de banda de potencia mitad, que quizás sea la definición más usual de ancho de banda. El ancho de banda de potencia mitad se define como el intervalo de frecuencias entre las cuales $S(f)$ ha caído a la mitad de la potencia máxima o, lo que es lo mismo, 3 dB por debajo del valor del pico.

B.3. LECTURAS RECOMENDADAS

En [JAME01] se ofrece un tratamiento del desarrollo de las series y transformadas de Fourier. Para profundizar en las series y transformadas de Fourier se recomienda el libro [KAMM00].

JAME01 James, J. *A Student's Guide to Fourier Transforms*. Cambridge, England: Cambridge University Press, 2001.

KAMM00 Kammler, D. *A First Course in Fourier Analysis*. Upper Saddle River, NJ: Prentice Hall, 2000.

APÉNDICE C

Programación de *sockets*

El concepto de *socket*, así como la programación de los *socket*s, fueron desarrollados en los años ochenta en el entorno de Unix como la interfaz de *socket*s de Berkeley. Básicamente, un *socket* permite la comunicación entre un proceso cliente y un proceso servidor y puede ser orientado a conexión o no orientado a conexión. Un *socket* puede considerarse como un punto final en una comunicación. Un *socket* cliente en una computadora utiliza una dirección para llamar a un *socket* servidor en otro computador. Una vez se han enlazado los *socket*s apropiados, los computadores pueden intercambiar datos.

Normalmente los computadores con *socket* servidores mantienen un puerto TCP o UDP abierto, preparado para llamadas de entrada eventuales. El cliente generalmente determina la identificación del *socket* del servidor deseado hallándolo en la base de datos de un sistema de nombres de dominio (DNS). Una vez establecida la conexión, el servidor conmuta el diálogo a un número de puerto diferente para liberar el número de puerto principal para llamadas de entrada adicionales.

Las aplicaciones de Internet, como TELNET y acceso remoto («rlogin»), hacen uso de los *socket*s, ocultando los detalles al usuario. No obstante, los *socket*s pueden crearse desde un programa (en un lenguaje como C o Java), permitiendo al programador proporcionar fácilmente funciones y aplicaciones de red. El mecanismo de programación de *socket* incluye una semántica suficiente como para permitir que se comuniquen dos procesos independientes en máquinas diferentes.

La interfaz de *socket* de Berkeley es el estándar de facto para interfaz de programación de aplicaciones (API) para el desarrollo de aplicaciones de red, extendiéndose en un amplio abanico de sistemas operativos. La API de *socket* proporciona acceso genérico a servicios de comunicación entre procesos. Así pues, la capacidad de los *socket*s es ideal para que los estudiantes aprendan los principios de los protocolos y aplicaciones distribuidas mediante el desarrollo de programas por ellos mismos.

La página web de este curso incluye un resumen general sobre la programación de *socket*s más enlaces a páginas con más información sobre el tema. Además, el manual del instructor incluye un conjunto de proyectos de programación.

APÉNDICE D

Proyectos para la enseñanza de comunicaciones de datos y redes de computadores

Un gran número de docentes cree que la investigación o la implementación de proyectos son cruciales para la comprensión clara de los conceptos de las comunicaciones y redes de computadores. Sin proyectos puede ser difícil para los estudiantes entender algunos de los conceptos básicos e interacciones entre componentes. Los proyectos refuerzan los conceptos presentados en el libro, ofrecen al estudiante una comprensión más amplia de cómo los protocolos y esquemas de transmisión funcionan y pueden motivar a los estudiantes y brindarles la confianza de que han dominado el material.

En este texto, he intentado presentar los conceptos tan claramente como ha sido posible y he propuesto unos 270 ejercicios y problemas para reforzar dichos conceptos. Muchos instructores desearán complementar este material con proyectos. Este apéndice proporciona orientación en ese respecto y describe el material de apoyo disponible en el manual del instructor. El material de soporte cubre cuatro tipos de proyectos:

- Proyectos de simulación.
- Proyectos de modelado del rendimiento.
- Proyectos de investigación.
- Trabajos de lecturas y elaboración de informes.

D.1. PROYECTOS DE SIMULACIÓN

La simulación de elementos clave ofrece una excelente forma de comprender el funcionamiento de los protocolos de comunicación y configuraciones de red, así como para estudiar y apreciar algunas de las cuestiones de diseño y sus implicaciones en el rendimiento. Una herramienta útil para este propósito es *cnet*.

Comparada con la implementación real software y hardware, la simulación proporciona diversas ventajas en los ámbitos de la investigación y educación:

- Mediante simulación es fácil modificar varios elementos de una configuración de red o varios elementos de un protocolo, para variar las características de rendimiento de distintos componentes y analizar después los efectos de dichas modificaciones.
- La simulación permite obtener estadísticas detalladas del funcionamiento, las cuales pueden utilizarse para comprender los compromisos de rendimiento.

La herramienta de simulación de red *cnet* [MCDO91] permite la experimentación con protocolos de nivel de enlace de datos, nivel de red y de nivel de encaminamiento y transporte, en varias configuraciones de red. Ha sido específicamente diseñado para cursos universitarios de redes de computadores y lo utilizan en todo el mundo por miles de estudiantes desde 1991.

El simulador *cnet* fue desarrollado por el Profesor Chris McDonald en la Universidad de Australia Occidental. El Profesor McDonald ha desarrollado un manual de usuario para el estudiante y un conjunto de proyectos específicos para su uso con este libro, que están disponibles para los profesores que los soliciten.

El simulador *cnet* se ejecuta en diversas plataformas UNIX y LINUX. El software puede descargarse desde la página web de *cnet*. Se encuentra disponible sin coste alguno para uso no comercial.

D.2. MODELADO DE RENDIMIENTO

Una alternativa a la simulación para evaluar el rendimiento de un sistema de comunicaciones o protocolo de red es el modelado analítico. Tal y como se emplea aquí, el modelado analítico se refiere a las herramientas para realizar análisis de colas, así como herramientas para realizar comprobaciones estadísticas simples sobre los datos de tráfico de red y herramientas para generar series temporales para el análisis.

El profesor Kenneth Christensen ha desarrollado un conjunto de potentes herramientas fáciles de usar en la Universidad del Sur de Florida. Su *página de herramientas* contiene herramientas relacionadas principalmente con la evaluación de redes de computadores y programación de *sockets* TCP/IP, que pueden ser descargadas. Cada herramienta está escrita en ANSI C. El formato para cada herramienta es el mismo, con una descripción de su propósito en la cabecera del programa, notas generales, ejemplos de entradas, ejemplos de salidas, instrucciones para su compilación, instrucciones para su ejecución, e información de contacto y sobre el autor. El código está documentado mediante extensos comentarios en línea y bloques de cabecera para todas las funciones. El objetivo de cada programa es la de servir como un instrumento de enseñanza para el concepto implementado por la herramienta (y como un modelo de buenas prácticas de programación). Por ello, su énfasis se centra en la claridad y simplicidad. Se asume que el estudiante tendrá acceso a un compilador de C y que tiene al menos una experiencia moderada programando en C.

El profesor Christensen ha desarrollado un manual de usuario para el estudiante y un conjunto de proyectos específicos para su uso con este libro. También están disponibles para los profesores que lo soliciten. El software puede descargarse desde la página web de las *herramientas*. Se encuentra disponible sin coste alguno para uso no comercial.

D.3. PROYECTOS DE INVESTIGACIÓN

Una forma efectiva de reforzar los conceptos básicos del curso y enseñar a los estudiantes metodologías de investigación consiste en encomendarles un proyecto de investigación. Un proyecto de este tipo podría implicar la búsqueda de bibliografía así como la localización en la web de productos comerciales, actividades de investigación de laboratorios y proposiciones de estandarización. Los proyectos pueden asignarse a grupos o, para proyectos pequeños, de forma individual. En cualquier caso, lo mejor es requerir algún tipo de propuesta inicial de proyecto, dando al instructor tiempo para evaluar lo apropiado del tema y la adecuación del nivel de esfuerzo de la propuesta. El trabajo previo del estudiante para los proyectos de investigación debe incluir:

- Un formato para la propuesta.
- Un formato para el informe final.
- Una programación con las fechas de las entregas final e intermedias.
- Una lista de posibles temas para el proyecto.

Los estudiantes pueden seleccionar uno de los temas listados o idear un proyecto comparable propio. El manual del instructor incluye un formato recomendado para la propuesta e informe final, además de una lista de posibles temas para la investigación.

D.4. TRABAJOS DE LECTURAS Y ELABORACIÓN DE INFORMES

Otra excelente manera de reforzar conceptos del curso y proporcionar a los estudiantes experiencia en la investigación es asignar artículos de la bibliografía para que sean leídos y analizados. El manual del instructor incluye una lista de artículos recomendados para que se asignen. Todos los artículos están disponibles vía Internet o en cualquier buena biblioteca técnica de universidad. El manual incluye además una recomendación sobre la redacción del trabajo.

Glosario

Algunas de las definiciones en este glosario proceden del *American Nacional Standard Dictionary of Information Technology* (diccionario estándar nacional de tecnología de la información), normalización ANSI X3.172, 1995. Estas definiciones están marcadas con un asterisco.

Acceso múltiple por demanda/asignación Técnica para asignar capacidad a un satélite, basada en FDM o en TDM, en la que la capacidad se concede según demanda.

Aloha Una técnica de control de acceso al medio para medios de transmisión de acceso múltiple. Una estación transmite siempre que tiene datos para enviar. Se repiten las transmisiones que no son confirmadas.

Amplitud El tamaño o magnitud de una onda de tensión o de corriente.

Ancho de banda* Diferencia entre las frecuencias límite (superior e inferior) de un espectro de frecuencias continuo.

Anillo con paso de testigo Técnica de control de acceso al medio para anillos. Un testigo circula sobre el anillo. Una estación puede transmitir capturando el testigo, insertando un paquete en el anillo y reponiendo el testigo.

Anillo Topología de red local en la que las estaciones están conectadas a repetidores conectados en un lazo cerrado. Los datos se transmiten en una dirección alrededor del anillo y pueden ser leídos por todas las estaciones conectadas a la red.

Arquitectura de comunicaciones La estructura hardware y software que implementan las funciones de comunicación.

Atenuación Disminución en amplitud de la corriente, tensión o potencia de una señal durante su transmisión entre puntos.

Autenticación* Proceso usado para verificar la integridad de los datos transmitidos, especialmente mensajes.

Banda ancha En general, equipos o sistemas de banda ancha que pueden transportar señales ocupando una gran porción del espectro electromagnético. Generalmente, un sistema de comu-

nicación en banda ancha puede acomodar simultáneamente voz, datos, vídeo y otros servicios. En los sistemas de transmisión digital, el término denota el uso de una alta tasa de datos.

Banda base Transmisión de señales sin modulación. En una red local de banda base, las señales digitales (unos y ceros) se insertan directamente en el cable como pulsos de tensión. Todo el espectro del cable es ocupado por la señal. Este esquema no permite multiplexación por división de frecuencia.

Baudio Unidad de velocidad de la señal, dada por el número de valores discretos o eventos de una señal por segundo o la inversa del tiempo de duración del elemento de señal más corto.

Bit de paridad* Un bit de comprobación añadido a un conjunto de dígitos binarios para hacer la suma de todos los dígitos binarios, incluyendo el bit de comprobación, siempre par (paridad par) o impar (paridad impar).

Bucle local Camino de transmisión, generalmente de par trenzado, entre el abonado individual y el centro de conmutación más cercano de la red pública de telecomunicaciones.

Bus* Uno o más conductores que sirven como conexión común para un grupo de dispositivos relacionados.

Bus con paso de testigo Técnica de control de acceso al medio para bus y árbol. Las estaciones forman un anillo lógico sobre el que se transfiere un testigo. La estación que recibe el testigo puede transmitir datos y después debe pasar el testigo a la estación siguiente en el anillo.

Byte Grupo de 8 bits, con el que normalmente se opera como una entidad.

Cabecera Información de control definida por el sistema que precede a los datos del usuario.

Cable coaxial Cable que contiene un conductor en su interior, normalmente un tubo o hilo de cobre, aislado por otro conductor de mayor diámetro, generalmente un tubo de cobre o cobre trenzado.

Capa* Grupo de servicios, funciones y protocolos, completo desde un punto de vista conceptual, que constituye uno de entre un conjunto de grupos dispuestos jerárquicamente y que se extiende a través de todos los sistemas que conforman la arquitectura de la red.

Capa de adaptación ATM (AAL, *ATM Adaptation Layer*) Capa que transforma los protocolos de transferencia de información en ATM.

Capa de aplicación Capa 7 del modelo OSI. Esta capa determina la interfaz del sistema con el usuario.

Capa de enlace de datos* En OSI, la capa que proporciona el servicio de transferencia de datos entre entidades de la capa de red, generalmente en nodos adyacentes. La capa de enlace de datos detecta y, potencialmente, corrige los errores que puedan ocurrir en la capa física.

Capa de presentación* Capa 6 del modelo OSI. Permite la selección de una sintaxis común para representar datos y para transformar datos de aplicación en y desde la sintaxis común.

Capa de red Capa 3 del modelo OSI. Responsable del encaminamiento de los datos a través de la red de comunicación.

Capa de sesión Capa 5 del modelo OSI. Gestiona una conexión lógica (sesión) entre dos procesos o aplicaciones que se comunican.

Capa de transporte Capa 4 del modelo OSI. Proporciona una transferencia de datos fiable y transparente entre puntos extremos.

Capa física Capa 1 del modelo OSI. Relacionada con aspectos eléctricos, mecánicos y de temporización de la transmisión de una señal en un medio.

CATV Televisión por cable (*Community Antenna Televisión*). El cable CATV se usa para redes locales de banda ancha y para distribución de emisiones de TV.

Cifrado* Convertir textos nativos o datos en una forma ininteligible mediante el uso de un código de forma que, posteriormente, se pueda hacer la reconversión a la forma original.

Cifrado asimétrico Un método de cifrado en el que el cifrado y el descifrado se realizan usando dos claves diferentes, una de ellas llamada clave pública y la otra clave privada. También se conoce como cifrado de clave pública.

Cifrado convencional Cifrado simétrico.

Cifrado de clave pública Cifrado asimétrico.

Cifrado simétrico Tipo de sistema criptográfico en el que el cifrado y descifrado se realizan usando la misma clave. También se conoce como cifrado convencional.

Circuito virtual Servicio de conmutación de paquetes en el que se establece una conexión (circuito virtual) entre dos estaciones al comienzo de la transmisión. Todos los paquetes siguen la misma ruta y llegan secuencialmente, no necesitando llevar una dirección completa.

Clave privada Una de las dos claves usadas en un sistema de cifrado asimétrico. Para que una comunicación sea segura, la clave privada debe ser conocida únicamente por su creador.

Clave pública Una de las dos claves usadas en un sistema de cifrado asimétrico. La clave pública se hace pública, para ser usada junto con su correspondiente clave privada.

***Codec* (codificador-decodificador)** Transforma datos analógicos en un flujo digital de bits (codificador) y señales digitales en datos analógicos (decodificador).

Codificación diferencial Un tipo de codificación de datos digitales en una señal digital o analógica de forma que el valor binario se determina por un cambio de la señal, en lugar de por el nivel de la misma.

Codificación Manchester Técnica de señalización digital en la que hay una transición en medio de cada intervalo de duración de un bit. Se codifica un 1 con un nivel alto durante la primera mitad del bit. Se codifica un 0 con un nivel bajo durante la primera mitad del bit.

Código de detección de errores* Código en el que cada secuencia se ajusta a reglas de construcción específicas de forma que, si ocurren ciertos errores en ella, la secuencia resultante no se ajuste a las reglas de construcción y, por tanto, se pueda detectar la presencia de errores.

Colisión Situación en la que dos paquetes se transmiten a través de un medio al mismo tiempo. Su interferencia hace a ambos ininteligibles.

Comprobación de redundancia cíclica Código de detección de errores en el que el código es el resto resultante de dividir los bits a comprobar entre un número binario predeterminado.

Comprobación de redundancia longitudinal Uso de un conjunto de bits de paridad para un bloque de caracteres de tal forma que hay un bit de paridad para cada posición de bit de los caracteres.

Conmutación de circuitos Método de comunicación en el que se establece un camino de comunicación entre dos dispositivos a través de uno o más nodos de conmutación intermedios. A diferencia de la conmutación de paquetes, los datos digitales se envían como una secuencia continua de bits. El ancho de banda está garantizado y el retardo está limitado esencialmente al retardo de propagación. El sistema telefónico utiliza conmutación de circuitos.

Conmutación de paquetes Método de transmisión de mensajes a través de una red de comunicación en la que los mensajes largos se subdividen en pequeños paquetes. Los paquetes se transmiten después como en conmutación de mensajes.

Conmutación por división espacial Técnica de conmutación de circuitos en la que cada conexión a través del conmutador toma un camino dedicado físicamente separado.

Conmutación por división temporal Técnica de conmutación de circuitos en la que los intervalos de tiempo en un flujo de datos multiplexado son asignados para transferir datos desde una entrada a una salida.

Conmutador digital Una red local con topología en estrella. Usualmente se refiere a un sistema que maneja sólo datos, pero no voz.

Contención Situación que se produce cuando dos o más estaciones intentan usar el mismo canal al mismo tiempo.

Control de acceso al medio (MAC, *Medium Access Control*) Para redes de difusión, método de determinación del dispositivo que tiene acceso al medio de transmisión en cada momento. Son métodos de acceso al medio CSMA/CD y paso de testigo.

Control de flujo Función realizada por una entidad receptora para limitar la cantidad o velocidad de los datos que una entidad transmisora envía.

CSMA (*Carrier Sense Multiple Access*, acceso múltiple con detección de portadora) Técnica de control de acceso al medio para medios de transmisión de acceso múltiple. Una estación que desee transmitir, comprueba el medio y sólo transmite si éste está desocupado.

CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*, acceso multiple con detección de portadora y detección de colisiones) Un refinamiento de CSMA en el que una estación cesa la transmisión si detecta una colisión.

Datagrama* En conmutación de paquetes, un paquete, independiente de los otros paquetes, que lleva información suficiente para su encaminamiento desde el equipo terminal de datos (DTE) de origen hasta el DTE de destino sin necesidad de establecer una conexión entre los DTE y la red.

Datos analógicos* Datos representados por una magnitud física que varía continuamente y cuya magnitud es directamente proporcional al dato o a la función que se ajusta a los datos.

Datos digitales Datos que consisten en una secuencia de valores discretos.

Decibelio Medida de la intensidad relativa de dos señales. El número de decibelios es 10 veces el logaritmo del cociente de la potencia de dos señales o 20 veces el logaritmo del cociente de la tensión de dos señales.

Densidad de potencia espectral (PSD, *Power Spectral Density*) La PSD de una señal es una función de la frecuencia que representa la potencia por unidad de ancho de banda de las componentes espectrales para cada frecuencia.

Descifrado La traducción de un texto o datos cifrados (llamado texto cifrado) al texto o datos originales (o texto nativo).

Diafonía* Fenómeno por el que una señal transmitida en un circuito o canal de un sistema de transmisión crea un efecto indeseado en otro circuito o canal.

Difusión Transmisión simultánea de datos a varias estaciones.

Digitalizar* Convertir una señal analógica en una señal digital.

Dirección de difusión Una dirección que designa todas las entidades en un dominio (por ejemplo, una red o Internet).

Dirección multidestino (*multicast*) Una dirección que designa a un grupo de entidades en un dominio (por ejemplo, una red o una interconexión de redes).

Dispersión (1) (fibra óptica) Cambio en la dirección de los rayos de luz después de golpear una o varias partículas pequeñas o debido a variaciones rápidas en la densidad del cristal. **(2) (propagación de ondas de radio)** Producción de ondas con la dirección o frecuencia modificadas cuando las ondas de radio inciden sobre la materia.

Dispositivo de encaminamiento o encaminador (*router*) Dispositivo de red que conecta dos redes de computadores. Usa un protocolo de interconexión de redes y asume que todos los dispositivos conectados a la red usan la misma arquitectura y protocolos de red. Un dispositivo de encaminamiento opera en la capa 3 de OSI.

Distorsión de retardo Distorsión de una señal que ocurre cuando el retardo de propagación del medio de transmisión no es constante en el rango de frecuencias de la señal.

Elemento de señal Parte de una señal que ocupa el intervalo temporal más corto de un código de señalización. Es el menor elemento reconocido en el receptor y puede corresponder a un único bit, a parte de un bit o a múltiples bits.

Encaminamiento Determinación del camino o ruta que atravesarán las unidades de datos (tramas, paquetes, mensajes, etc.) desde la fuente al destino.

Encapsulado Adición de información de control por una entidad de protocolo sobre datos obtenidos de un usuario del protocolo.

Equipo de terminación de red Agrupación de funciones RDSI en la frontera entre RDSI y el abonado.

Equipo terminación del circuito de datos (DCE, *Data Circuit-terminating Equipment*) En una estación de datos, el equipo que proporciona la conversión de señales y la codificación entre el equipo terminal de datos (DTE, *Data terminal equipment*) y la línea. El DCE puede ser un equipo independiente o una parte integrada en el DTE o en un equipo intermedio. El DCE puede realizar otras funciones que normalmente se realizan en el extremo de la red de la línea.

Equipo terminal de datos (DTE, *Data Terminal Equipment*)* Equipo consistente en instrumentos finales digitales que convierten la información del usuario en señales de datos para transmisión o reconvierten las señales de datos recibidas en información de usuario.

Espectro Rango absoluto de frecuencias. Por ejemplo, el espectro del cable CATV, en la actualidad, comprende de 5 a 400 MHz.

Estrella Topología en la que todas las estaciones están conectadas a un conmutador central. Dos estaciones se comunican por medio de conmutación de circuitos.

Fase Para una señal periódica $f(t)$, la parte fraccionaria, t/P, del periodo, P, que se ha desplazado t respecto de un origen arbitrario. El origen se toma habitualmente en el último paso por cero desde valores negativos a positivos.

Fibra óptica Filamento fino de cristal u otro material transparente a través del que se puede transmitir, mediante reflexión total interna, un haz de luz de una señal codificada.

Firma digital Mecanismo de autenticación que habilita al creador de un mensaje a adjuntar un código que actúa como firma. La firma garantiza la fuente y la integridad del mensaje.

Frecuencia Velocidad de oscilación de la señal en hercios.

Función de dispersión (*hash*) Función que asigna a un bloque de datos de longitud variable o a un mensaje un valor de longitud fija llamado código de dispersión. La función se diseña de forma que, cuando está protegida, se puede usar como autenticación de los datos o de los mensajes. También se denomina resumen del mensaje.

HDLC (*High-level Data Link Control*, control del enlace de datos de alto nivel) Protocolo de enlace de datos (capa 2 de OSI) orientado a bits muy común, definido por ISO. Los protocolos LAPB, LAPD y LLC son similares.

Incorporación de confirmación (*piggybacking*) Inclusión de una confirmación de un paquete previamente recibido en un paquete de datos saliente.

Información de control del protocolo* Información intercambiada entre entidades de una capa dada, por medio del servicio proporcionado por la capa inmediatamente inferior, para coordinar su funcionamiento conjunto.

Interconexión de redes Comunicación entre dispositivos a través de varias redes.

Medio de transmisión Camino físico entre transmisores y receptores en un sistema de comunicación.

Microondas Ondas electromagnéticas en el rango de frecuencias entre 2 y 40 GHz.

Modelo de referencia para la interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*) Modelo de comunicación entre dispositivos que cooperan. Define una arquitectura de siete capas de funciones de comunicación.

Módem (modulador/demodulador) Transforma un flujo de bits digitales en una señal analógica (modulador) y viceversa (demodulador).

Modo de transferencia asíncrono (ATM, *Asynchronous Transfer Mode*) Un método de transmisión de paquetes, llamados celdas, usando un tamaño de paquete fijo. ATM es la interfaz de transferencia de datos para RDSI-BA. A diferencia de X.25, ATM no proporciona mecanismos de control de errores ni de control de flujo.

Modulación* Proceso o resultado del proceso de variación de algún parámetro de una señal, llamada portadora, de acuerdo con una señal mensaje.

Modulación angular* Modulación en la que se varía el ángulo de una onda portadora senoidal. La modulación en fase y en frecuencia son formas particulares de modulación angular.

Modulación de amplitud* Una forma de modulación en la que la amplitud de la onda portadora varía de acuerdo con alguna característica de la señal modulante.

Modulación de fase Modulación en la que el ángulo de fase de una portadora es el parámetro que se varía.

Modulación de frecuencia Modulación en la que la frecuencia de una señal sinusoidal alterna es el parámetro que se varía.

Modulación por código de pulso Proceso en el que se muestrea una señal y se cuantiza la magnitud de cada muestra según una referencia prefijada, codificándola en una señal digital.

Modulación por desplazamiento de amplitud Modulación en la que los dos valores binarios se representan con dos amplitudes diferentes de la frecuencia de la portadora.

Modulación por desplazamiento de fase Modulación en la que la fase de la señal portadora se desplaza para representar datos digitales.

Modulación por desplazamiento de frecuencia Modulación en la que los dos valores binarios se representan con dos frecuencias diferentes próximas a la frecuencia de la portadora.

Multiplexación por división en el tiempo estadística Método de TDM en el que los intervalos de tiempo, en una línea de transmisión compartida, se sitúan en canales de E/S bajo demanda.

Multiplexación por división en el tiempo síncrona Método TDM en el que los intervalos de tiempo de una línea de transmisión compartida son asignados a canales de E/S de forma fija y predeterminada.

Multiplexación por división en el tiempo División de un servicio de transmisión en dos o más canales transmitiendo la información de cada uno de ellos en intervalos de tiempo diferentes.

Multiplexación por división en frecuencias División de un medio de transmisión en dos o más canales fraccionando la banda de frecuencia utilizada en la transmisión en bandas más estrechas y usando cada una de ellas como un canal diferente.

Multiplexación En transmisión de datos, una función que permite a dos o más fuentes de datos compartir un medio de transmisión común de tal forma que cada fuente de datos tiene su propio canal.

Multipunto Configuración en la que más de dos estaciones comparten un camino de transmisión.

Notación de sintaxis abstracta 1 (ASN.1) Un lenguaje formal usado para definir una sintaxis. En el caso de SNMP, la notación ASN.1 se usa para definir el formato de las unidades de datos y objetos del protocolo SNMP.

Número de saltos El número de saltos a lo largo de un camino desde una fuente dada a un destino dado es igual al número de nodos de la red (nodos de conmutación de paquetes, conmutadores ATM, enrutadores, etc.) que un paqete se encuentra a lo largo de dicho camino.

Octeto Grupo de ocho bits, con el que usualmente se opera como una entidad.

Onda periódica Una onda $f(t)$ que satisface $f(t) = f(t + nk)$ para todo entero n, siendo k una constante.

Paquete Grupo de bits que incluye datos e información adicional de control. Generalmente se refiere a una unidad de datos del protocolo de la capa de red (capa 3 de OSI).

Par trenzado Medio de transmisión que consta de dos cables aislados dispuestos según un patrón regular en forma de espiral.

Parada y espera Protocolo de control de flujo en el que la estación emisora transmite un bloque de datos y espera una confirmación antes de transmitir el siguiente bloque.

PBX (*Private Branch Exchange*) Centralita privada. Una centralita de teléfono bajo el control del usuario. Proporciona un servicio de conmutación para teléfonos en líneas de extensión dentro de un edificio y acceso a la red telefónica pública.

Periodo Valor absoluto del mínimo intervalo tras el que se obtienen los mismos valores de una onda periódica.

Portadora común En los Estados Unidos, las compañías que ofrecen servicios de comunicaciones al público. La aplicación usual es proporcionar servicios de telecomunicación de larga distancia. Las portadoras comunes son reguladas por las comisiones de regulación federales y estatales.

Portadora Frecuencia continua capaz de ser modulada o readaptada por una segunda señal (portadora de información).

Protocolo Internet Protocolo de interconexión de redes que proporciona servicios sin conexión a través de múltiples redes de conmutación de paquetes.

Protocolo Conjunto de reglas que gobiernan la operación de unidades funcionales para llevar a cabo la comunicación.

Puente* Unidad funcional que interconecta dos redes de área local (LAN) que usan el mismo protocolo de control de enlace lógico, pero que pueden usar distintos protocolos de control de acceso al medio.

Punto a punto Configuración en la que dos estaciones comparten una ruta de transmisión.

Punto de acceso al servicio (SAP, *Service Access Point*) Una manera de identificar a un usuario de servicios de una entidad de protocolo. Una entidad de protocolo proporciona uno o más SAP para uso de las entidades del nivel superior.

RDSI de banda ancha (RDSI-BA) Segunda generación de RDSI. La característica clave de RDSI de banda ancha es que proporciona canales de transmisión capaces de soportar velocidades mayores que la velocidad primaria RDSI.

Red de área local de banda ancha Uso de cable coaxial para proporcionar una transferencia de datos mediante señales analógicas (de radiofrecuencia). Las señales digitales se adaptan en un módem y se transmiten en una de las bandas de frecuencia del cable.

Red de área local Red de comunicación que proporciona interconexión entre varios dispositivos de comunicación de datos en un área pequeña.

Red de comunicación conmutada Red de comunicación formada por una red de nodos conectados por enlaces punto a punto. Los datos se transmiten desde la fuente al destino a través de nodos intermedios.

Red de comunicación de difusión Red de comunicaciones en la que la transmisión emitida por una estación es recibida por todas las demás estaciones.

Red de comunicación Colección de unidades funcionales interconectadas que proporcionan servicios de comunicación de datos entre estaciones conectadas a la red.

Red de valor añadido Red de paquetes conmutados privada cuyos servicios se ofertan al público.

Red digital de servicios integrados (RDSI) Servicio de telecomunicación mundial que usa transmisión y tecnología de conmutación digitales para realizar comunicaciones de datos digitales y de voz.

Red pública de datos Una red de paquetes conmutados de monopolio nacional o controlada por el gobierno. Este servicio está disponible públicamente para procesar datos de los usuarios.

Redes interconectadas Conjunto de redes de conmutación de paquetes y de difusión que están interconectadas mediante encaminadores.

Relleno de bits La inserción de bits extra en una cadena de datos para evitar la aparición de secuencias de control no deseadas.

Repetidor Dispositivo que recibe datos sobre un enlace de comunicaciones y los transmite, bit a bit, sobre otro enlace tan rápido como se reciben los datos, sin utilizar almacenamiento temporal.

Retardo de propagación Retardo entre el momento en el que una señal entra al canal y el instante en que se recibe.

Retransmisión de celdas (*cell relay*) Mecanismo de conmutación de paquetes usado para los paquetes de tamaño fijo llamados celdas. ATM se basa en la tecnología de retransmisión de celdas.

Retransmisión de tramas (*frame relay*) Una forma de conmutación de paquetes basada en el uso de tramas de la capa de enlace de longitud variable. No hay capa de red y muchas de las funciones básicas se descartan o eliminan para proporcionar mayor rendimiento.

Ruido blanco Ruido que presenta un espectro plano o uniforme en el rango de frecuencias de interés.

Ruido de intermodulación Ruido debido a la combinación no lineal de señales de frecuencias diferentes.

Ruido impulsivo Pulso de ruido de gran amplitud y corta duración.

Ruido térmico Ruido estadísticamente uniforme que depende de la temperatura del medio de transmisión.

Ruido Señales no deseadas que se combinan con la señal transmitida o recibida y que, por tanto, la distorsionan.

Secuencia de comprobación de trama Código de detección de errores insertado como campo en el bloque de datos a transmitir. El código sirve para comprobar la existencia de errores cuando se reciben los datos.

Señal analógica Onda electromagnética que varía continuamente y se puede propagar por medios diversos.

Señal digital Señal discreta o discontinua como, por ejemplo, un conjunto de pulsos de tensión.

Señal limitada en banda Una señal en la que toda la energía está contenida en un rango de frecuencias finito.

Señalización por canal común Técnica en la que las señales de control de la red (por ejemplo, una solicitud de llamada) se separan de las señales de voz o datos asociadas, ubicando la señalización asociada a un grupo de señales de voz o de datos en un canal separado dedicado únicamente a señalización.

Señalización Intercambio de información relacionada con el establecimiento y control de las conexiones y con su gestión en una red de telecomunicación.

Sin retorno a cero Técnica de señalización digital en la que la señal permanece en un nivel constante durante la duración completa de un bit.

Sistema intermedio (IS, *Intermediate System*) Dispositivo conectado a dos o más subredes en una interconexión de redes y que realiza encaminamiento y retransmisión de datos entre sistemas extremos. Ejemplos de sistemas intermedios son los puentes y los encaminadores.

Solicitud de repetición automática Una característica que inicia automáticamente una petición de una retransmisión cuando se detecta un error en la transmisión.

Sondeo y selección Proceso mediante el cual una estación primaria sondea a las estaciones secundarias, una a una, invitándolas a transmitir (sondeo) o solicita a una secundaria recibir datos (selección).

Suma de comprobación (*checksum*) Código de detección de errores basado en la suma de los bits que se van a comprobar.

Tasa de bits erróneos Probabilidad de que un bit transmitido se reciba con error.

Tasa de error residual Tasa de error restante después de intentar la corrección de los mismos.

Tasa de errores* Cociente entre el número de unidades de datos erróneas y el número total de unidades de datos.

Técnicas de ventana deslizante Método de control de flujo en el que una estación que transmite puede enviar paquetes numerados dentro de un intervalo de números (ventana). La ventana cambia dinámicamente para permitir que se envíen paquetes adicionales.

Telemática Servicios de transmisión de información orientados a usuario. Incluye teletexto, videotexto y fax.

Texto cifrado La salida de un algoritmo de cifrado. La forma cifrada de un mensaje o dato.

Texto nativo La entrada de una función de cifrado o la salida de una función de descifrado.

Topología Estructura, compuesta por enlaces y conmutadores, que proporciona el medio de interconexión entre los nodos de la red.

Trama Grupo de bits que incluye datos, una o más direcciones y otra información de control de protocolo. Generalmente, se refiere a la unidad de datos del protocolo de la capa de enlace (capa 2 de OSI).

Transferencia de datos no orientada a conexión Protocolo para intercambio de datos de una manera no planeada y sin coordinación previa (por ejemplo, datagrama).

Transferencia de datos orientada a conexión Protocolo para intercambio de datos en el que se establece una conexión lógica entre los puntos extremos (por ejemplo, un circuito virtual).

Transmisión analógica La transmisión de señales analógicas independientemente de su contenido. La señal se puede amplificar, pero no hay intentos intermedios de recuperar los datos de la señal.

Transmisión asíncrona Transmisión en la que cada carácter de información se sincroniza individualmente (normalmente usando elementos de inicio y parada).

Transmisión balanceada Modo de transmisión en el que las señales se transmiten como una corriente que viaja a través de un conductor y vuelve por otro. Para señales digitales, esta técnica se conoce como señalización diferencial y el valor binario viene determinado por una diferencia de tensión.

Transmisión digital Transmisión de datos digitales, usando tanto señales analógicas como digitales, en la que los datos digitales se recuperan y repiten en puntos intermedios para reducir los efectos del ruido.

Transmisión en modo corriente Modo de transmisión en el que el transmisor aplica corriente alternativamente a cada uno de los dos conductores de un par trenzado para representar el 1 o 0 lógicos. La corriente total es constante y siempre en la misma dirección.

Transmisión *full-duplex* Transmisión de datos en ambas direcciones al mismo tiempo.

Transmisión *half-duplex* Transmisión de datos en cualquier dirección, pero sólo una dirección en un instante de tiempo.

Transmisión no balanceada Modo de transmisión en el que las señales se transmiten por un único conductor. Transmisor y receptor comparten una tierra común.

Transmisión *simplex* Transmisión de datos únicamente en una dirección preasignada.

Transmisión síncrona Transmisión de datos en la que el tiempo de ocurrencia de cada señal que representa un bit está relacionado con una referencia de tiempo fija.

Unidad de datos del protocolo (PDU, *Protocol Data Unit*)* Conjunto de datos especificado en un protocolo de una capa dada y que consta de información de control del protocolo de esa capa y, posiblemente, de datos del usuario de esa capa.

Bibliografía

ABREVIATURAS

ACM Association for Computing Machinery
IEEE Institute of Electrical and Electronics Engineers
NIST National Institute of Standards and Technology

10GE02 10 Gigabit Ethernet Alliance. *10 Gigabit Ethernet-Technology Overview*. White Paper, abril 2002.

ADAM91 Adamek, J. *Foundations of Coding*. New York: Wiley, 1991.

ANDE95 Anderson, J.; Rappaport, T.; y Yoshida, S. «Propagation Measurements and Models for Wireless Communications Channels.» *IEEE Communications Magazine*, enero 1995.

ANDR99 Andrikopoulos, I.; Liakopoulous, A.; Pavlou, G.; y Sun, Z. «Providing Rate Guarantees for Internet Application Traffic Across ATM Networks.» *IEEE Communications Surveys*, tercer cuatrimestre 1999. http://www.comsoc.org/pubs/surveys.

ARMI93 Armitage, G., y Adams, K. «Packet Reassembly During Cell Loss.» *IEEE Network*, septiembre 1995.

ARMI00 Armitage, G. *Quality of Service in IP Networks*. Indianapolis, en: Macmillan Technical Publishing, 2000.

ASH90 Ash, R. *Information Theory*. New York: Dover, 1990.

BANT94 Bantz, D., y Bauchot, F. «Wireless LAN Design Alternatives.» *IEEE Network*, marzo/abril, 1994.

BELL00 Bellamy, J. *Digital Telephony*. New York: Wiley, 2000.

BELL90 Bellcore (Bell Communications Research). *Telecommunications Transmission Engineering*, volumen 2: Facilities. 1990.

BENE64 Benice, R. «An Analysis of Retransmission Systems.» *IEEE Transactions on Communication Technology*, diciembre 1964.

BERG91 Bergman, W. «Narrowband Frame Relay Congestion Control.» *Proceedings of the Tenth Annual Phoenix Conference of Computers and Communications*, marzo 1991.

BERG96 Bergmans, J. *Digital Baseband Transmission and Recording*. Boston: Kluwer, 1996.

BERL87 Berlekamp, E.; Peile, R.; y Pope, S. «The Application of Error Control to Communications.» *IEEE Communications Magazine*, abril 1987.

BERN00 Bernet, Y. «The Complementary Roles of RSVP and Differentiated Services in the Full-Service QoS Network.» *IEEE Communications Magazine*, febrero 2000.

BERT92 Bertsekas, D., y Gallager, R. *Data Networks.* Englewood Cliffs, NJ: Prentice Hall, 1992.

BERT94 Bertoni, H.; Honcharenko, W.; Maciel, L.; y Xia, H. «UHF Propagation Prediction for Wireless Personal Communications.» *Proceedings of the IEEE*, septiembre 1994.

BHAR83 Bhargava, V. «Forward Error Correction Schemes for Digital Communications.» *IEEE Communications Magazine*, enero 1983.

BHAT97 Bhatnagar, P. *Engineering Networks for Synchronization, CCS 7 and ISDN.* New York: IEEE Press, 1997.

BLAC93 Black, U. *Data Link Protocols.* Englewood Cliffs, NJ: Prentice Hall, 1993.

BLAC95 Black, U. *The V Series Recommendations: Standards for Data Communications Over the Telephone Network.* New York: McGraw-Hill, 1996.

BLAC96 Black, U. *Physical Level Interfaces and Protocols.* Los Alamitos, CA: IEEE Computer Society Press, 1996.

BLAC97 Black, U. *ISDN and SS7: Architectures for Digital Signaling Networks.* Upper Saddle River, NJ: Prentice Hall, 1997.

BLAC99a Black, U. *ATM Volume I: Foundation for Broadband Networks.* Upper Saddle River, NJ: Prentice Hall, 1992.

BLAC99b Black, U. *Second-generation Mobile and Wireless Networks.* Upper Saddle River, NJ: Prentice Hall, 1999.

BLAC00 Black, U. *IP Routing Protocols: RIP, OSPF, BGP, PNNI & Cisco Routing Protocols.* Upper Saddle River, NJ: Prentice Hall, 2000.

BORE97 Borella, M., et al., «Optical Components for WDM Lightwave Networks.» *Proceedings of the IEEE*, agosto 1997.

BOSS98 Bosse, J. *Signaling in Telecommunication Networks.* New York: Wiley, 1998.

BREY99 Breyer, R., y Riley, S. *Switched, Fast, and Gigabit Ethernet.* New York: Macmillan Technical Publishing, 1999.

BUCK00 Buckwalter, J. *Frame Relay: Technology and Practice.* Reading, MA: Addison-Wesley, 2000.

BURG91 Burg, J., y Dorman, D. «Broadband ISDN Resource Management: The Role of Virtual Paths.» *IEEE Communications Magazine*, septiembre 1991.

BUX80 Bux, W.; Kummerle, K.; y Truong, H. «Balanced HDLC Procedures: A Performance Analysis.» *IEEE Transactions on Communications*, noviembre 1980.

CARN99 Carne, E. *Telecommunications Primer: Data, Voice, and Video Communications.* Upper Saddle River, NJ: Prentice Hall, 1999.

CARP02 Carpenter, B., y Nichols, K. «Differentiated Services in the Internet.» *Proceedings of the IEEE*, septiembre 2002.

CERT03 CERT Coordination Center. *CERT Coordination Center 2002 Annual Report.* Carnegie-Mellon University, 2003. http://www.cert.org/annual_rpts/cert_rpt_02.html.

CLAR92 Clark, D.; Shenker, S.; y Zhang, L. «Supporting Real-Time Applications in an Integrated Services Packet Network: Architecture and Mechanism» *Proceedings, SIGCOMM '92*, agosto 1992.

CLAR95 Clark, D. *Adding Service Discrimination to the Internet.* MIT Laboratory for Computer Science Technical Report, septiembre 1995. Disponible en http://ana-www.lcs.mit.edu/anaWeb/papers.html.

CLAR98 Clark, D., y Fang, W. «Explicit Allocation of Best-Effort Packet Delivery Service.» *IEEE/ACM Transactions on Networking*, agosto 1998.

COME99 Comer, D., y Stevens, D. *Internetworking with TCP/IP, Volume II: Design Implementation, and Internals.* Upper Saddle River, NJ: Prentice Hall, 1994.

COME00 Comer, D. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture.* Upper Saddle River, NJ: Prentice Hall, 2000.

COME01 Comer, D., y Stevens, D. *Internetworking with TCP/IP, Volume III: Client-Server Programming and Applications.* Upper Saddle River, NJ: Prentice Hall, 2001.

CORM01 Cormen, T., et al., *Introduction to Algorithms.* Cambridge, MA: MIT Press, 2001.

COUC01 Couch, L. *Digital and Analog Communication Systems.* Upper Saddle River, NJ: Prentice Hall, 2001.

CROW97 Crow, B., et al., «IEEE 802.11 Wireless Local Area Networks.» *IEEE Communications Magazine*, septiembre 1997.

DAVI89 Davies, D., y Price, W. *Security for Computer Networks.* New York: Wiley, 1989.

DIFF76 Diffie, W., y Hellman, M. «Multiuser Cryptographic Techniques.» *IEEE Transactions on Information Theory*, noviembre 1976.

DIJK59 Dijkstra, E. «A Note on Two Problems in Connection with Graphs.» *Numerical Mathematics*, octubre 1959.

DINA98 Dinan, E., y Jabbari, B. «Spreading Codes for Direct Sequence CDMA and Wideband CDMA Cellular Networks.» *IEEE Communications Magazine*, septiembre 1998.

DIXO94 Dixon, R. *Spread Spectrum Systems with Commercial Applications.* New York: Wiley, 1994.

DUTT99 Dutta-Roy, A. «Cable: It's Not Just for TV.» *IEEE Spectrum*, mayo 1999.

EFF98 Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design.* Sebastopol, CA: O'Reilly, 1998.

FCIA98 Fibre Channel Industry Association. *Fibre Channel Storage Area Networks.* San Francisco: Fibre Channel Industry Association, 2001.

FIOR95 Fiorini, D.; Chiani, M.; Tralli, V.; y Salati, C. «Can We Trust HDLC?» *Computer Communications Review*, octubre 1995.

FORD62 Ford, L. y Fulkerson, D. *Flows in Networks.* Princeton, NJ: Princeton University Press, 1962.

FRAZ99 Frazier, H., y Johnson, H. «Gigabit Ethernet: From 100 to 1,000 Mbps.» *IEEE Internet Computing*, enero/febrero 1999.

FREE96 Freeman, R. *Telecommunication System Engineering.* New York: Wiley, 1996.

FREE97 Freeman, R. *Radio System Design for Telecommunications.* New York: Wiley, 1997.

FREE98a Freeman, R. *Telecommunication Transmission Handbook.* New York: Wiley, 1998.

FREE98b Freeman, R. «Bits, Symbols, Baud, and Bandwidth.» *IEEE Communications Magazine*, abril 1998.

FREE99 Freeman, R. *Fundamentals of Telecommunications.* New York: Wiley, 1999.

FREE02 Freeman, R. *Fiber-Optic Systems for Telecommunications.* New York: Wiley, 2002.

GARR96 Garrett, M. «A Service Architecture for ATM: From Applications to Scheduling.» *IEEE Network*, mayo/junio 1996.

GEIE99 Geier, J. *Wireless LANs.* New York: Macmillan Technical Publishing, 1999.

GEIE01 Geier, J. «Enabling Fast Wireless Networks with OFDM.» *Communications System Design*, febrero 2001. (www.csdmag.com)

GERS91 Gersht, A. y Lee, K. «A Congestion Control Framework for ATM Networks.» *IEEE Journal on Selected Areas in Communications*, septiembre 1991.

GIBS93 Gibson, J. *Principles of Digital and Analog Communications.* New York: Macmillan, 1993.

GIBS97 Gibson, J. ed. *The Communications Handbook.* Boca Raton, FL: CRC Press, 1997.

GIRA90 Girard, A. *Routing and Dimensioning in Circuit-switching Networks.* Reading, MA: Addison-Wesley, 1990.

GLOV98 Glover, I., y Grant, P. *Digital Communications.* Upper Saddle River, NJ: Prentice Hall, 1998.

GOYA98 Goyal, R., et al., «Providing Rate Guarantees to TCP over the ATM GFR Service.» *Proceedings of the Local Computer Networks Conference*, octubre 1998.

HAAS00 Haas, Z. «Wireless and Mobile Networks.» En [TERP00].

HARB92 Harbison, R. «Frame Relay: Technology for Our Time.» *LAN Technology*, diciembre 1992.

HARJ00 Harju, J., y Kivimaki, P. «Cooperation and Comparison of DiffServ and IntServ: Performance Measurements.» *Proceedings, 23rd Annual IEEE Conference on Local Computer Networks*, noviembre 2000.

HATA80 Hata, M. «Empirical Formula for Propagation Loss in Land Mobile Radio Services.» *IEEE Transactions on Vehicular Technology*, marzo 1980.

HAWL97 Hawley, G. «Systems Considerations for the Use of xDSL Technology for Data Access.» *IEEE Communications Magazine*, marzo 1997.

HAYK01 Haykin, S. *Communication Systems.* New York: Wiley, 2001.

HIND83 Hinden, R., Haverty, J. y Sheltzer, A. «The DARPA Internet: Interconnecting Heterogeneous Computer Networks with Gateways.» *Computer*, septiembre 1983.

HIND95 Hinden, R. «IP Next Generation Overview.» *Connexions*, marzo 1995.

HUIT98 Huitema, C. *IPv6: The New Internet Protocol.* Upper Saddle River, NJ: Prentice Hall, 1998.

HUIT00 Huitema, C. *Routing in the Internet.* Upper Saddle River, NJ: Prentice Hall, 2000.

HUMP97 Humphrey, M., y Freeman, J. «How xDSL Supports Broadband Services to the Home.» *IEEE Network*, enero/marzo 1997.

HURW98 Hurwicz, M. «Fibre Channel: More Vision Than Reality?» *Network Magazine*, junio 1998.

JACO88 Jacobson, V. «Congestion Avoidance and Control.» *Proceedings*, *SIGCOMM '*88, *Computer Communication Review*, agosto 1988; reimpreso en *Computer Communication Review*, enero 1995; una versión ligeramente modificada está disponible en ftp.ee.lbl.gov/papers/congavoid.ps.Z.

JACO90 Jacobson, V. «Berkeley TCP Evolution from 4.3 Tahoe to 4.3-Reno.» *Proceedings of the Eighteenth Internet Engineering Task Force*, septiembre 1990.

JAIN91 Jain, R. *The Art of Computer Systems Performance Analysis*: *Techniques for Experimental Design*, *Measurement*, *Simulation*, *and Modeling*. New York: Wiley, 1991.

JAIN92 Jain, R. «Myths About Congestion Management in High-Speed Networks.» *Internetworking*: *Research and Experience*, vol. 3, 1993.

JAME01 James, J. *A Student's Guide to Fourier Transforms*. Cambridge, England: Cambridge University Press, 2001.

JOHN98 Johnston, M. *An Up-to-Date Review of Physical Layer Measurements*, *Cabling Standards*, *Troubleshooting Practices*, *and Certification Techniques*. Phoenix, AZ: Microtest Inc. 1998.

KADA98 Kadambi, J.; Crayford, I.; y Kalkunte, M. *Gigabit Ethernet*. Upper Saddle River, NJ: Prentice Hall, 1998.

KAMM00 Kammler, D. *A First Course in Fourier Analysis*. Upper Saddle River, NJ: Prentice Hall, 2000.

KARN91 Karn, P., y Partridge, C. «Improving Round-Trip Estimates in Reliable Transport Protocols.» *ACM Transactions on Computer Systems*, noviembre 1991.

KHAN89 Khanna, A., y Zinky, J. «The Revised ARPANET Routing Metric.» *Proceedings*, *SIGCOMM '*89 *Symposium*, 1989.

KAHN97 Kahn, J., y Barry, J. «Wireless Infrared Communications.» *Proceedings of the IEEE*, febrero 1997.

KESH98 Keshav, S., y Sharma, R. «Issues and Trends in Router Design.» *IEEE Communications Magazine*, mayo 1998.

KILK99 Kilkki, K. *Differentiated Services for the Internet*. Indianapolis, IN: Macmillan Technical Publishing, 1999.

KLEI76 Kleinrock, L. *Queuing Systems*, *Volume II*: *Computer Applications*. New York: Wiley, 1976.

KLEI92 Kleinrock, L. «The Latency/Bandwidth Tradeoff in Gigabit Networks.» *IEEE Communications Magazine*, abril 1992.

KLEI93 Kleinrock, L. «On the Modeling and Analysis of Computer Networks.» *Proceedings of the IEEE*, agosto 1993.

KNUT98 Knuth, D. *The Art of Computer Programming*, *Volume* 2: *Seminumerical Algorithms*. Reading, MA: Addison-Wesley, 1998.

KONH80 Konheim, A. «A Queuing Analysis of Two ARQ Protocols.» *IEEE Transactions on Communications*, julio 1980.

KRIS01 Krishnamurthy, B., y Rexford, J. *Web Protocols and Practice*: *HTTP*/1.1, *Networking Protocols*, *Caching*, *and Traffic Measurement*. Upper Saddle River, NJ: Prentice Hall, 2001.

KUMA98 Kumar, V.; Lakshman, T.; y Stiliadis, D. «Beyond Best Effort: Router Architectures for the Differentiated Services of Tomorrow's Internet.» *IEEE Communications Magazine*, mayo 1998.

KURO01 Kurose, J., y Ross, K. *Computer Networking*. Reading, MA: Addison-Wesley, 2001.

LARO02 LaRocca, J., y LaRocca, R. 802.11 *Demystified*. New York: McGraw-Hill, 2002.

LEBO98 Lebow, I. *Understanding Digital Transmission and Recording*. New York: IEEE Press, 1998.

LEON00 Leon-Garcia, A., y Widjaja, I. *Communication Networks*: *Fundamental Concepts and Key Architectures*. New York: McGraw-Hill, 2000.

LEUT94 Leutwyler, K. «Superhack.» *Scientific American*, julio 1994.

LIN84 Lin, S.; Costello, D; y Miller, M. «Automatic-Repeat-Request Error-Control Schemes.» *IEEE Communications Magazine*, diciembre 1984.

LUIN97 Luinen, S., Budrikis, Z.; y Cantoni, A. «The Controlled Cell Transfer Capability.» *Computer Communications Review*, enero 1997.

MAXW96 Maxwell, K. «Asymmetric Digital Subscriber Line: Interim Technology for the Next Forty Years.» *IEEE Communications Magazine*, octubre 1996.

MCDO91 McDonald, C. «A Network Specification Language and Execution Environment for Undergraduate Teaching.» *Proceedings of the ACM Computer Science Educational Technical Symposium*, marzo 1991.

MCDY99 McDysan, D., y Spohn, D. *ATM*: *Theory and Application*. New York: McGraw-Hill, 1999.

MCQU80 McQuillan, J., Richer, I. y Rosen, E. «The New Routing Algorithm for the ARPANET.» *IEEE Transactions on Communications*, mayo 1980.

METZ99 Metzler, J., y DeNoia, L. *Layer* 2 *Switching*. Upper Saddle River, NJ: Prentice Hall, 1999.

MOSH89 Moshos, G. *Data Communications*: *Principles and Problems*. New York: West Publishing Co., 1989.

MOY98 Moy, J. *OSPF*: *Anatomy of an Internet Routing Protocol*. Reading, MA: Addison-Wesley, 1998.

OHAR99 Ohara, B., y Petrick, A. *IEEE* 802.11 *Handbook*: *A Designer's Companion*. New York: IEEE Press, 1999.

OJAN98 Ojanpera, T., y Prasad, G. «An Overview of Air Interface Multiple Access for IMT-2000/UMTS.» *IEEE Communications Magazine*, septiembre 1998.

OKUM68 Okumura, T., et. al., «Field Strength and Its Variability in VHF and UHF Land Mobile Radio Service.» *Rev. Elec. Communication Lab*. 1968.

PAHL95 Pahlavan, K.; Probert, T.; y Chase, M. «Trends in Local Wireless Networks.» *IEEE Communications Magazine*, marzo 1995.

PARK88 Park, S., y Miller, K. «Random Number Generators: Good Ones are Hard to Find.» *Communications of the ACM*, octubre 1988.

PARE88 Parekh, S., y Sohraby, K. «Some Performance Trade-Offs Associated with ATM Fixed-Length Vs. Variable-Length Cell Formats.» *Proceedings*, *GlobeCom*, noviembre 1988.

PEAR92 Pearson, J. *Basic Communication Theory*. Englewood Cliffs, NJ: Prentice Hall, 1992.

PERL00 Perlman, R. *Interconnections*: *Bridges*, *Routers*, *Switches*, *and Internetworking Protocols*. Reading, MA: Addison-Wesley, 2000.

PETE95 Peterson, R.; Ziemer, R.; y Borth, D. *Introduction to Spread Spectrum Communications*. Englewood Cliffs, NJ: Prentice Hall, 1995.

PETE61 Peterson, W., y Brown, D. «Cyclic Codes for Error Detection.» *Proceedings of the IEEE*, enero 1961.

PETE00 Peterson, L., y Davie, B. *Computer Networks*: *A Systems Approach*. San Francisco: Morgan Kaufmann, 2000.

PICK82 Pickholtz, R.; Schilling, D.; and Milstein, L. «Theory of Spread Spectrum Communications-A Tutorial.» IEEE Transactions on Communications, mayo 1982. Reimpreso en [TANT98].

PRAS98 Prasad, R., y Ojanpera, T. «An Overview of CDMA Evolution: Toward Wideband CDMA.» *IEEE Communications Surveys*, cuarto trimestre 1998. Disponible en www.comsoc.org.

PRAS00 Prasad, R.; Mohr, W.; y Konhauser, W., eds. *Third-Generation Mobile Communication Systems*. Boston: Artech House, 2000.

PROA02 Proakis, J. *Communication Systems Engineering*. Upper Saddle River, NJ: Prentice Hall, 2002.

RAMA88 Ramabadran, T., y Gaitonde, S. «A Tutorial on CRC Computations.» *IEEE Micro*, agosto 1988.

RAPP96 Rappaport, T. *Wireless Communications*. Upper Saddle River, NJ: Prentice Hall, 1996.

RAPP97 Rappaport, T.; Rias, M.; y Kapoor, V. «Propagation Models.» En [GIBS97].

REEV95 Reeve, W. *Subscriber Loop Signaling and Transmission Handbook*. Piscataway, NJ: IEEE Press, 1995.

RIVE78 Rivest, R.; Shamir, A.; y Adleman, L. «A Method for Obtaining Digital Signatures and Public Key Cryptosystems.» *Communications of the ACM*, febrero 1978.

RODR02 Rodriguez, A., et al., *TCP/IP Tutorial and Technical Overview*. Upper Saddle River: NJ: Prentice Hall, 2002.

ROSE98 Rose, M., y Strom, D. *Internet Messaging*: *From the Desktop to the Enterprise*. Upper Saddle River, NJ: Prentice Hall, 1998.

RUSS95 Russell, R. *Signaling System Á* 7. New York: McGraw-Hill, 1995.

SACH96 Sachs, M., y Varma, A. «Fibre Channel and Related Standards.» *IEEE Communications Magazine*, agosto 1996.

SATO90 Sato, K.; Ohta, S.; y Tokizawa, I. «Broad-Band ATM Network Architecture Based on Virtual Paths.» *IEEE Transactions on Communications*, agosto 1990.

SATO91 Sato, K.; Ueda, H.; y Yoshikai, M. «The Role of Virtual Path Crossconnection.» *IEEE LTS*, agosto 1991.

SCHN96 Schneier, B. *Applied Cryptography*. New York: Wiley, 1996.

SEIF98 Seifert, R. *Gigabit Ethernet*. Reading, MA: Addison-Wesley, 1998.

SEIF00 Seifert, R. *The Switch Book*. New York: Wiley, 2000.

SHEN95 Shenker, S. «Fundamental Design Issues for the Future Internet.» *IEEE Journal on Selected Areas in Communications*, septiembre 1995.

SING99 Singh, S. *The Code Book*: *The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor Books, 1999.

SKLA93 Sklar, B. «Defining, Designing, and Evaluating Digital Communication Systems.» *IEEE Communications Magazine*, noviembre 1993.

SKLA01 Sklar, B. *Digital Communications*: *Fundamentals and Applications*. Upper Saddle River, NJ: Prentice Hall, 2001.

SPOH02 Spohn, D. *Data Network Design*. New York: McGraw-Hill, 2002.

SPUR00 Spurgeon, C. *Ethernet*: *The Definitive Guide*. Cambridge, MA: O'Reilly and Associates, 2000.

SPRA91 Spragins, J.; Hammond, J.; y Pawlikowski, K. *Telecommunications*: *Protocols and Design*. Reading, MA: Addison-Wesley, 1991.

STAL99a Stallings, W. *ISDN and Broadband ISDN*, *with Frame Relay and ATM*. Upper Saddle River, NJ: Prentice Hall, 1999.

STAL99b Stallings, W. *SNMP*, *SNMPv*2, *SNMPv*3, *and RMON* 1 *and* 2. Reading, MA: Addison-Wesley, 1999.

STAL00 Stallings, W. *Local and Metropolitan Area Networks*, 6*th ed*. Upper Saddle River, NJ: Prentice Hall, 2000.

STAL02 Stallings, W. *Wireless Communications and Networks*. Upper Saddle River, NJ: Prentice Hall, 2002.

STAL03 Stallings, W. *Cryptography and Network Security*: *Principles and Practice*, 3*rd ed*. Upper Saddle River, NJ: Prentice Hall, 2003.

STEI95 Steinke, S. «IP Addresses and Subnet Masks.» *LAN Magazine*, octubre 1995.

STEV94 Stevens, W. *TCP/IP Illustrated*, *Volume* 1: *The Protocols*. Reading, MA: Addison-Wesley, 1994.

STEV96 Stevens, W. *TCP/IP Illustrated*, *Volume* 3: *TCP for Transactions*, *HTTP*, *NNTP*, *and the UNIX(R) Domain Protocol*. Reading, MA: Addison-Wesley, 1996.

SUZU94 Suzuki, T. «ATM Adaptation Layer Protocol.» *IEEE Communications Magazine*, abril 1995.

TANE03 Tanenbaum, A. *Computer Networks*. Upper Saddle River, NJ: Prentice Hall, 2003.

TANT98 Tantaratana, S, y Ahmed, K., eds. *Wireless Applications of Spread Spectrum Systems*: *Selected Readings*. Piscataway, NJ: IEEE Press, 1998.

TERP00 Terplan, K., y Morreale, P. eds. *The Telecommunications Handbook*. Boca Raton, FL: CRC Press, 2000.

TSUD92 Tsudik, G. «Message Authentication with One-Way Hash Functions.» *Proceedings*, *INFOCOM'*92, mayo 1992.

WALR98 Walrand, J. *Communication Networks*: *A First Course*. New York: McGraw-Hill, 1998.

WALR00 Walrand, J., y Varaiya, P. *High-Performance Communication Networks*. San Francisco, CA: Morgan Kaufmann, 2000.

WANG92 Wang, Z., and Crowcroft, J. «SEAL Detects Cell Misordering.» *IEEE Network*, julio 1992.

WEIS98 Weiss, W. «QoS with Differentiated Services.» *Bell Labs Technical Journal*, octubre-diciembre 1998.

WHIT97 White, P., y Crowcroft, J. «The Integrated Services in the Internet: State of the Art.» *Proceedings of the IEEE*, diciembre 1997.

WIDM83 Widmer, A. y Franaszek, P. «A DC-Balanced, Partitioned, 8B/10B Transmission Code.» *IBM Journal of Research and Development*, septiembre 1983.

WRIG95 Wright, G., y Stevens, W. *TCP/IP Illustrated*, *Volume* 2: *The Implementation*. Reading, MA: Addison-Wesley, 1995.

WILL97 Willner, A. «Mining the Optical Bandwidth for a Terabit per Second.» *IEEE Spectrum*, abril 1997.

XIAO99 Xiao, X., y Ni, L. «Internet QoS: A Big Picture.» *IEEE Network*, marzo/abril 1999.

XION00 Xiong, F. *Digital Modulation Techniques*. Boston: Artech House, 2000.

ZENG00 Zeng, M.; Annamalai, A.; y Bhargava, V. «Harmonization of Global Third-Generation Mobile Systems. *IEEE Communications Magazine*, diciembre 2000.

ZHAN86 Zhang, L. «Why TCP Timers Don't Work Well.» *Proceedings*, *SIGCOMM '*86 *Symposium*, agosto 1986.

ZHAN93 Zhang, L.; Deering, S.; Estrin, D.; Shenker, S.; y Zappala, D. «RSVP: A New Resource ReSerVation Protocol.» *IEEE Network*, septiembre 1993.

ZHAN95 Zhang, H. «Service Disciplines for Guaranteed Performance Service in Packet-Switching Networks.» *Proceedings of the IEEE*, octubre 1995.

ZORZ96 Zorzi, M., y Rao, R. «On the Use of Renewal Theory in the Analysis of ARQ Protocols.» *IEEE Transactions on Communications*, septiembre 1996.

Índice

1000BASE-CX, 528
1000BASE-LX, 528
1000BASE-SX, 528
1000BASE-T, 528
100BASE-T4, 525-526
100BASE-X, 525
10BASE2, 523
10BASE5, 523
10BASE-F, 523
10BASE-T, 523
10BASE-T, especificaciones del medio, 523
3G América, 474
4B/5B-NRZI, 543-545
8B10B, 548
8B6T, 546-548
  tabla de código, 547

A

abonados, red pública de telecomunicaciones, 314
absorción atmosférica, 124, 125
acceso múltiple por demanda/asignación, 821
acceso múltiple por división de código (CDMA, *Code Division Multiple Access*), 286, 287
  aspectos de diseño, 472-473
    ancho de banda, 472
    multitasa, 472
    tasa de minibits, 472
  para espectro expandido de secuencia directa, 299-300
  principios básicos, 297-299
acceso remoto (*rlogin*), 814
acondicionamiento del tráfico, 436
acuerdo de nivel de servicio (SLA, *Service Level Agreement*), 666
adquisición de vecinos, 646
ADSL universal, 280
Agencia de Proyectos de Investigación Avanzados para la Defensa (DARPA, *Defense Advanced Research Projects Agency*), 40
agrupamiento, capa de sesión, 39
alcance de direccionamiento, 594
alcance de radio, 109
alcanzabilidad de los vecinos, 646
Alcatel, 257
alfabeto de referencia internacional (IRA, *International Reference Alfabet*), 72
algoritmo de Bellman-Ford, 398-400
algoritmo de cifrado de clave pública RSA, 745-747
  ejemplo, 746
algoritmo de descifrado, 727, 744
algoritmo de dispersión seguro (SHA, *Secure Hash Algoritm*), 740
algoritmo de encaminamiento de tercera generación, 394-396
algoritmo de Jacobson, 709-713
algoritmo de Karn, 713-714
algoritmo del árbol de expansión, 501, 503-504
algoritmos de cifrado, 727, 744
  estándar de cifrado avanzado (AES, *Advanced Encryption Standard*), 729-732
  estándar de cifrado de datos (DES, *Data Encryption Standard*), 728-729
algoritmos de encaminamiento de mínimo coste, 397-401
  algoritmo de Bellman-Ford, 398-400
  algoritmo de Dijkstra, 397-398
  comparación, 401
algoritmos de encaminamiento de primera generación, 392-393

algoritmos de encaminamiento de segunda generación, 393-394
Alianza de Ethernet a 10 Gigabits, 540
ALOHA, 516-517, 821
Aloha ranurado, 516, 517
  amplitud, 134, 821
  amplitud de pico, 60
análisis de Fourier, 809-810
  representación mediante la transformada de Fourier de señales no periódicas, 810-813
    densidad de potencia espectral y ancho de banda, 810-813
  representación mediante series de Fourier de señales periódicas, 809-810
ancho de banda, 65, 83, 96, 821
  efecto sobre una señal digital, 68
  relación entre velocidad de transmisión y, 66-69
ancho de banda absoluto, 65
ancho de banda efectivo, 65
anillo, 821
anillo de paso de testigo, 530-534, 821
  anillo de paso de testigo dedicado (DTR, *Dedicated Token Ring*), 534
  control de acceso al medio (MAC, *Medium Access Control*), 532-534
  definición, 530
  funcionamiento del anillo, 530-532
  opciones de medios de transmisión en IEEE 802.5, 534
  principales desventajas, 534
  repetidores, 530-531
ANSI, 59
antena isotrópica, 110
antena parabólica de reflexión, 110-111
antenas, 110-11
  área efectiva de una, 111
  ganancia, 110-111
antenas de microondas, 112
aplicabilidad global, 594
aplicación entre redes, conexión de camino virtual (VPC, *Virtual Path Connection*), 430-432
aplicación usuario-red, conexión de camino virtual, 431
aplicación usuario-usuario, conexión de camino virtual, 431
aplicaciones distribuidas, 763-806
  correo electrónico, 764-780
  gestión de red, 794-805
  MIME (*MultipurposeInternet Mail Extension*, extensiones multipropósito de correo electrónico), 764, 772-780
  protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*), 780-794
    caché, 784
    campos de la cabecera general, 786
    elementos, 787
    entidades, 793-794
    mensajes, 784-786
    mensajes de respuesta, 790-793
    mensajes de solicitud, 786-790
    pasarela, 783
    representante, 782-783
    túnel, 784
    visión general, 780-786
  protocolo simple de transferencia de correo electrónico (SMTP, *Simple Mail Transfer Protocol*), 764-772
aprendizaje de direcciones, 503
Área de Seguridad del IETF, 759
área efectiva, antenas, 111
aritmética módulo 2, 185-188
armónico fundamental, 809
armónicos, 809
ARPANET, 40, 390-393, 395, 418, 644
  algoritmo de encaminamiento de primera generación, 392-393
  algoritmo de encaminamiento de segunda generación, 393-394
  algoritmo de encaminamiento de tercera generación, 394-396
  métricas de retardo, 396
ARQ de parada y espera, 224-225
ARQ de rechazo selectivo, 228-229
ARQ vuelta atrás N, 226-228
ARQ, *véase* solicitud de retransmisión automática
arquitectura de protocolos, 21-52
  canal de fibra, 537
  capa de acceso a la red, 25, 31
  capa de aplicación, 25, 31
  capa de transporte, 25, 31
  definición, 22-24
  gestión de red, 797-798
  IEEE 802.11, 574
  modelo de referencia para la interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*), 29-39
  modo de transferencia asíncrona (ATM, *Asynchronous Transfer Mode*), 350
  necesidad de, 22-23
  puentes, 499-500
  puntos de acceso al servicio (SAP, *Service Access Point*), 25
  redes de área local (LAN, *Local Area Network*), 489-497
  retransmisión de tramas, 342-343
    plano de control, 342
    plano de usuario, 343

simple, 23-29
TCP/IP, 40-45
unidad de datos del protocolo (PDU, *Protocol Data Unit*), 27
arquitectura de servicios diferenciados, 632
arquitectura de servicios integrados (ISA, *Integrated Services Architecture*), 632, 654-665
aproximación, 657-658
componentes, 658-659
agente de gestión, 659
control de admisión, 658
protocolo de encaminamiento, 659
disciplina de cola, 662-663
encaminador:
clasificador y selección de ruta, 659
gestor de la cola de salida, 659
retransmisión de paquetes, 659
funciones de congestión, 658
protocolo de reserva de recursos (RSVP, *Resource Reservation Protocol*), 665
características, 665
estado temporal, 665
multidifusión, 665
unidifusión, 664
servicios, 659-662
especificación de tráfico mediante cubo de testigos, 660-661
servicio garantizado, 660-661
servicios de carga controlada, 662
tráfico de internet, 655-656
tráfico elástico, 655-656
tráfico inelástico, 656-657
arquitectura *softswitch*, 329
ASCII, 72
ASK, *véase* modulación por desplazamiento de amplitud (ASK)
Asociación de Industrias de Canal de Fibra (*Fibre Channel Industry Association*), 535
Asociación de Industrias de Redes de Almacenamiento, 540
Asociación de LAN Inalámbricas (*Wireless LAN Alliance*), 582
asociación de telecomunicaciones celulares e Internet, 474
asociaciones de seguridad (SA, *Security Associations*), 755
dirección IP de destino, 755
identificador del protocolo de seguridad, 756
índice de parámetros de seguridad (SPI, *Security Parameters Index*), 755
parámetros, 756
AT&T, 256, 263, 314, 380
ataque por fuerza bruta, 728
ataques activos, 726
ataques de denegación de servicio, 726
ataques pasivos, 725-726
análisis de tráfico, 725
divulgación del contenido de un mensaje, 725
atenuación, 78-80, 821
ATM, *véase* modo de transferencia asíncrono (ATM)
audio, 70
ausencia de ambigüedad global, 594
autenticación, 821

B

banda ancha, 821
banda base, 822
banda lateral inferior, 165
banda lateral residual (VSB, *Vestigial Sideband*), 166
banda lateral superior, 165
banda lateral única (SSB, *Single Side Band*), 165
bandas de frecuencia, 118
barrido, 71
base de datos de información de gestión (MIB, *Management Information Base*), 804
base de datos de reenvío, 502
baudio, 822
BGP, *véase* protocolo de pasarela fronteriza (BGP)
binaria multinivel, 140-141
bipolar con sustitución de 8 ceros (B8ZS, *Bipolar with 8-Zeros Sustitution*), 144-145
bipolar de alta densidad de tres ceros (HDB3, *High Density Bipolar-3 zeros*), 145
bit de indicación usario ATM a usuario ATM (AAU), 357
bit de paridad, 822
bit de señalización, 264
bits de código, 543
bits de comprobación, 184
bits de sobrecarga de STS-1, 267
bucle local, 314
bucle remoto, 204
bucles de abonado, 99, 314
bus, 822
bus con paso de testigo, 822
byte, 822

C

cabecera, 822
PDU de acceso a la red, 27
PDU de transporte, 27
cabecera de autenticación, 756-758
cabecera de encaminamiento, IPv6, 626-627

cabecera de fragmento, IPv6, 626
cabecera de opciones salto a salto, 624-626
  campos, 624
  opciones, 624
cabecera de paquete, 44
cabecera IPv6, 620-623
  campo cabecera siguiente, 621
  campo clase de tráfico, 621
  campo dirección de destino, 621
  campo dirección origen, 621
  campo etiqueta de flujo, 621
  campo límite de saltos, 621
  campo longitud de la carga útil, 621
  campo versión, 621
  campos, 620
cabecera TCP, 43
cable coaxial, 59, 104, 148, 256, 822
  aplicaciones, 104
  banda ancha, 488
  banda base, 488
  características de transmisión, 104-105
  descripción física, 104
cableado de cobre de redes locales de alto rendimiento, alternativas, 103
cableado UTP, categorías, 101
caché, 784
caminos virtuales:
  características, 354-355
  terminología, 354
  ventajas, 352
campo de control de errores de cabecera, 358
campo de control de flujo genérico (GFC), 356, 359
campo de control, HDLC, 230-232
campo de dirección, 344
  de HDLC, 230
campo de información, HDLC, 232
campo de protección del número de secuencia (SNP, *Secuence Number Protection*), 372
campos de indicación, HDLC, 231-232
campos de indicación y secuencia de comprobación de trama (FCS), 344
canal, 251
canal de fibra, 535-539
  arquitectura de protocolos, 537
  Asociación de Industrias de Canal de Fibra (*Fibre Channel Industry Association*), 535
  comparación con las redes IEEE802, 536
  diseño, 535
  elementos, 536
  estructura, 536
    topología, 538
  medio de transmisión, 537-538
  medio físico, 537-538
  nodos, 536
  previsiones, 539
  recursos orientados a red incorporados, 535
  requisitos, 535-536
  topología en bucle arbitrado, 538
  topología punto a punto, 538
  topologías, 538
canal de fibra, topología en bucle arbitrado, 538
canal de metaseñalización, 356
canal virtual:
  calidad de servicio, 354
  características, 354-355
  conexiones de canal virtual conmutadas/semipermanentes, 355
  integridad de la secuencia de celdas, 355
  negociación y monitorización de los parámetros de tráfico, 355
  restricciones de identificador en un VPC, 355
  usos de la conexión, 353-354
canal virtual de señalización usuario-red, 356
canal virtual de señalización usuario-usuario, 356
canales, 259
canales del transpondedor, 113
cancelación de eco, 198, 276
capa, 822
capa de acceso a la red, 25
  TCP/IP, 40
capa de acceso al medio, Gigabit Ethernet, 526-530
capa de adaptación ATM (AAL, *ATM Adaptation Layer*), 350-351, 822
capa de aplicación:
  modelo de referencia para la interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*), 25, 30-32, 39, 826
  TCP/IP, 40
capa de control de enlace lógico (LLC, *Logical Link Control*), 37, 491
capa de enlace de datos, 30,-32, 37, 822
capa de presentación, 31, 39, 822
capa de red, 31, 36-39, 822
capa de sesión, 31, 39, 822
capa de *sockets* segura (SSL, *Secure Sockets Layer*), 724, 749-754
  arquitectura, 749-750
  protocolo de alerta, 752
  protocolo de cambio de especificación de cifrado, 751-752
  protocolo de negociación bilateral, 752-754
    fase 1, 752
    fase 2, 752
    fase 3, 753
    fase 4, 753
  protocolo de registro, 750-751

capa de transporte:
modelo de referencia para la interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*), 31, 38, 826
TCP/IP, 40-41
capa de transporte segura (TLS, *Transport Layer Security*), 749
capa extremo a extremo (capa de transporte), TCP/IP, 41
capa física:
Gigabit Ethernet, 528-529
modelo de referencia para la interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*), 29-32, 36, 490, 826
TCP/IP, 40-41
capa física basada en celdas, 362-364
capa física basada en SDH, 364-365
capacidad del canal, 83-87
ancho de banda de Nyquist, 84
ecuación de la capacidad de Shannon, 84-86
relación entre la energía de la señal por bit y la densidad de potencia del ruido, 86-87
capas pares, 23
caracteres de control, 72
características de procedimiento, capa física, 37
características de transmisión:
cable coaxial, 104-105
fibra óptica, 105-109
par trenzado, 99-101
radiodifusión, 116-117
características eléctricas, capa física, 36
características funcionales, capa física, 37
características mecánicas, capa física, 36
CATV (televisión por cable, *Community AntennaTelevisión*), 822
CBR, *véase* velocidad constante (CBR)
CDMA de banda ancha (W-CDMA, *Wideband CDMA*), 471-472
parámetros, 471
CDMA, *véase* acceso múltiple por división de código (CDMA)
celdas, 350
ATM, 356-361
campo de control de errores de cabecera, 358
campo de control de flujo genérico (GFC, *Generic Flow Control*), 356, 359
control de errores de cabecera, 360-361
control de flujo genérico, 358-359
formato de cabecera, 356-358
identificador de camino virtual (VPI, *virtual path identifier*), 357
identificador de canal virtual (VCI, *Virtual Channel Identifier*), 357
prioridad de pérdida de celdas (CLP, *Cell Loss Priority*), 358
tipo de carga útil (PT, *Payload Type*), 357
central de conmutación de telecomunicaciones móviles (MTSO, *Mobile Telecommunications Switching Office*), 451-454, 461
aceptación de la llamada, 453
bloqueo de llamadas, 454
corte de llamadas, 454
inicialización de la unidad móvil, 452
llamada en curso, 454
llamada originada en un móvil, 452
llamadas a/desde suscriptores fijos y móviles, 454
localización, 452
terminación de llamadas, 454
traspaso, 454
central del abonado, 314-315
centrales, red pública de telecomunicaciones, 314
centralita privada (PBX, *Private Branch Exchange*), 99, 313
Centro de Recursos de Retransmisión de Tramas, 346
certificado de clave pública, 748
cifrado, 726-735, 823
estándar de cifrado avanzado (AES, *Advanced Encryption Standard*), 726, 729-732
cifrado asimétrico, 823
cifrado de clave pública, 742-744, 823
algoritmo de cifrado de clave pública RSA, 745-747
ejemplo, 746
elementos, 743
gestión de claves, 748-749
pasos, 744
cifrado simétrico, 727-728, 823
algoritmo de cifrado
estándar de cifrado avanzado (AES, *Advanced Encryption Standard*), 729-732
estándar de cifrado de datos (DES, *Data Encryption Standard*), 728-729
algoritmo de descifrado, 727, 728-729
análisis criptográfico, 727
ataque por fuerza bruta, 728
clave secreta, 727
componentes, 727
distribución de claves, 733-735
relleno de tráfico, 735
requisitos, 727
texto cifrado, 727
texto nativo, 727
ubicación de los dispositivos de cifrado, 732-733
circuito troncal metropolitano, 106
circuito virtual, 353-354
circuitos de intercambio, 199
circuitos del bucle de abonado, 106
clave de sesión, 734
clave permanente, 734
clave privada, 743, 823
clave pública, 743, 823

clave secreta, 727
CM Special Interest Group on Communications (SIGCOMM), 3
COAST, 759
codec (codificador-decodificador), 76, 157, 823
codificación diferencial, 139, 823
codificación Manchester diferencial, 142, 181
codificación mediante inversión de pulso alternante (AMI, *Alternate Mark Inversion*), 278
código de detección de errores, 823
  cabecera de la PDU de transporte, 27
código de usuario, 297
código Manchester, 141-143, 143, 181, 199, 823
códigos bifase, 141-143
códigos ortogonales, 298
colisión, 516, 823
Comité de Estándares LAN/MAN de IEEE 802, 510
Comité Técnico de IEEE sobre Seguridad y Privacidad, 759
Compañía Siemon, 127
complejidad, lógica digital, 139
componente continua, 65, 809
comportamiento salto a salto, 672-674
  PHB de reenvío asegurado, 673-674
  PHB de reenvío urgente, 672-673
comprobación de paridad, 184-185
comprobación de redundancia cíclica (CRC, *Cyclic Redundancy Check*), 185-191, 372, 823
  aritmética módulo 2, 185-188
  lógica digital, 189-191
  polinomios, 188-189
comprobación de redundancia longitudinal, 823
comunicaciones de datos, 9-19
  configuración de ejemplo, 18-19
  definición, 13
  modelo de comunicaciones, 10-13
  y multiplexación, 251
concentrador raíz (HHUB), 505
concentradores, 488, 504-505
concentradores intermedios (IHUB), 505
conceptos en el dominio del tiempo, 59-62
  amplitud de pico, 60
  fase, 60
  frecuencia, 60
  longitud de onda, 62
  periodo, 60
  señal analógica, 59
  señal digital, 60
  señal no periódica, 60
  señal periódica, 60
conexión de camino virtual (VPC, *Virtual Path Connection*), 430-433
conexiones de canal virtual (VCC, *Virtual Channel Connection*), 351, 430-432
configuración de línea, 197-198
  topología, 197
  transmisión *full-duplex*, 197-198
  transmisión *half-duplex*, 197
configuración del encaminamiento estático, desarrollo, 501
configuración guiada multipunto, 59
confirmación negativa y retransmisión, 224
confirmación no numerada (UA, *Unnumbered Acknowledged*), 234
confirmación positiva, 224
congestión, 407-443
congestión en retransmisión de tramas, 418-424
  estrategia de rechazo, 419
  gestión de la tasa de tráfico, 420-423
  gestión de la velocidad del tráfico, 420-423
  prevención de congestión, 419
    con señalización explícita, 420
  recuperación de congestión, 420
  señalización explícita, 420
  señalización implícita, 420
  técnicas, 419, 423-424
  control, 12, 413-416
    contrapresión, 414
    en redes de conmutación de paquetes, 418
    paquete de obstrucción, 414-415
    señalización explícita de congestión, 415-416
    señalización implícita de congestión, 415
  efectos, 409-413
    rendimiento ideal, 410-412
    rendimiento real, 412-413
  gestión de tráfico, 416-418
    calidad de servicio (QoS, *Quality of Service*), 417
    imparcialidad, 417
    reservas, 417-418
  gestión de tráfico en ATM, 424-436
    efectos de la latencia/velocidad, 424-425
    requisitos, 424-425
    técnicas, 430-436
    variación del retardo de celda, 426-429
  gestión de tráfico en GFR, 436-439
    contrato de tráfico GFR, 436-439
    definición de adecuación GFR, 438-439
    etiquetado, 438
    gestión de las memorias temporales, 438
    mecanismo de comprobación de elegibilidad QoS, 439
    planificación, 438
    política, 438
    trama adecuada pero no elegible, 439
    trama adecuada y elegible, 439
    trama no adecuada, 439
conmutación de circuitos, 15, 309-348, 823
  arquitectura de conmutación lógica, 329-330

conmutación por división espacial, 317-319
conmutación por división temporal, 319
conmutador digital, 316
desventajas, 330
direccionamiento, 321
información de llamada, 321
interfaz de red, 316
señalización de control, 319-329
funciones de señalización, 320-321
señalización en canal común, 322-326
sistema de señalización número 7 (SS7), 326-329
ubicación de la señalización, 322
supervisión, 321
unidad de control, 316-317
conmutación de paquetes, 15, 309-348, 823
comparación con conmutación de circuitos, 336-339
rendimiento, 336-337
retardo de propagación, 336
retardo en el nodo, 336
tiempo de transmisión, 336
mediante circuitos virtuales, 336, 338
mediante datagramas, 336-337
principios, 330-339
retransmisión de tramas, 341-345
arquitectura de protocolos, 342-343
fundamentos, 341-342
transferencia de datos de usuario, 343-345
tamaño de paquete, 334-336
técnica de conmutación, 331-334
aproximación de circuito virtual, 334
aproximación de datagrama, 331
ventajas frente a conmutación de circuitos, 331
X.25, 339-341
conmutación por división en el tiempo, 823
conmutación por división espacial, 823
conmutador de almacenamiento y envío, 507
conmutador digital, 824
conmutador rápido, 507
conmutadores de capa 2, 504-507
conmutadores de capa 3, 508-509
consideraciones de diseño de CDMA móvil inalámbrico, 463-464
receptor RAKE, 463-464
Consorcio Internacional de *Softswitch*, 346
Consorcio WWW, 805
contención, 496, 824
contrapresión, 414
contrato de tráfico GFR, 436-439
control de acceso al medio (MAC, *Medium Access Control*), 491, 495-497, 824
contención, 496
formato de trama MAC, 496-497
IEEE 802.11, 572-579
control de acceso, 573-577
entrega de datos fiable, 572-573
función de coordinación distribuida (DFC, *Distributed Coordination Function*), 573-577
función de coordinación puntual, 577
trama MAC, 577-579
tramas de control, 578-579
tramas de datos, 579
tramas de gestión, 579
paso de testigo en anillo, 532-534
reserva, 496
rotación circular, 495-496
control de acceso al medio en IEEE 802.3,
ALOHA, 516-517
CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*, acceso múltiple con detección de portadora y detección de colisiones), 519-521
precursores, 516-519
trama MAC, 522
control de admisión de conexiones, 430
control de disparidad, 548
control de enlace de datos de alto nivel (HDLC, *High Level Data Link Control*), 37, 217, 229-236, 825
características básicas, 229-230
configuración balanceada, 229
configuración no balanceada, 229
estación combinada, 229
estación primaria, 229
estación secundaria, 229
modo asíncrono balanceado (ABM, *Asynchronous Balanced Mode*), 229
modo de respuesta asíncrono (ARM, *Asynchronous Response mode*), 229
modo de respuesta normal (NRM, *Normal Response Mode*), 229
estructura de trama, 230-233
cabecera, 230
campo de control, 232
campo de dirección, 232
campo de información, 232
campo de secuencia de comprobación de trama (FCS), 233
campos de delimitación, 231
cola, 230
funcionamiento, 233-236
desconexión, 237
ejemplos, 238-239
inicialización, 234
transferencia de datos, 237
órdenes y respuestas, 233
control de enlace de datos, definición, 216
control de errores, 223-229, 260, 592-593
definición, 223

interconexión de redes no orientada a conexión, 608
solicitud de repetición automática (ARQ, *Automatic Repeat Request*), 224-229
ARQ de parada y espera, 224-225
ARQ de rechazo selectivo, 228-229
ARQ vuelta atrás N, 226-227
técnicas comunes, 224
trama dañada, 224
trama perdida, 223
control de errores de cabecera, 360-361
control de flujo, 12, 217-223, 260, 592, 824
definición, 217
interconexión de redes no orientada a conexión, 608
control de flujo de parada y espera, 218-220, 241-243
control de flujo de ventana deslizante, 220-223, 824
cuestiones de rendimiento, 241-248
ARQ, 245-248
control de flujo de parada y espera, 241-243
control de flujo de ventana deslizante sin errores, 243-245
control de flujo de ventana deslizante libre de errores, 243-248
control de flujo genérico (GFC, *Generic Flow Control*), 358-359
control de los parámetros de uso (UPC, *Usage Parameter Control*), 434-435
control del enlace lógico (LLC, *Logical Link Control*), 491, 492-495
protocolo, 493-495
operación tipo 1, 494
operación tipo 2, 494
operación tipo 3, 495
servicios, 492-493
servicio en modo conectado, 492
servicio no orientado a conexión con confirmación, 492
servicio no orientado a conexión no confirmado, 492
control del enlace TDM, 260-263
delimitación de tramas, 261
inserción de pulsos, 262
controlador pasarela de medios (MGC, *Media Gateway Controller*), 330
corrección de errores, 178, 191-197
principios de los códigos de bloque, 193-197
corrección de errores hacia adelante, 459
correo electrónico, 764-780
coste, lógica digital, 139
CRC, *véase* comprobación de redundancia cíclica (CRC)
criptoanálisis, 727
CSMA (*Carrier Sense Multiple Access*, acceso múltiple con detección de portadora), 517, 824
no persistente, 518
CSMA no persistente, 518
CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*, acceso múltiple con detección de portadora y detección de colisiones), 519-521, 824
cubierta, fibra óptica, 105
Christensen, Kenneth, 818

D

datagrama, 824
datagrama IP, 44
datos analógicos, 69-72, 824
datos, definición, 69
datos digitales, 69-72, 75-76, 824
dBm (decibelio-milivatio), 93
dBW (decibelio-vatio), 93
DCE, *véase* equipo terminación del circuito de datos (DCE)
decibelio, 824
definición de adecuación GFR, 438-439
delimitación por dígitos añadidos, 261
demanda agregada de pico, conexión de camino virtual (VPC, *Virtual Path Connection*), 432
densidad de potencia espectral (PSD, *Power Spectral Density*), 810-813, 824
DES, *véase* estándar de cifrado de datos (DES)
descrifrado, 824
descripción física:
cable coaxial, 104
fibra óptica, 105
par trenzado, 99
radiodifusión, 116-117
destino, modelo de comunicaciones, 11
desvanecimiento, 456-459
corrección de errores hacia adelante, 459
difracción, 456
dispersión, 456
diversidad, 459
diversidad en frecuencias, 459
diversidad espacial, 459
ecualización adapativa, 459
mecanismos de compensación de errores, 459
propagación multitrayectoria, 456-457
efectos, 457-458
reflexión, 456
tipos, 458-459
desvanecimiento lento, 458
desvanecimiento plano, 458
desvanecimiento rápido, 458
desvanecimiento selectivo, 458
detección de errores, 138, 178, 183-191
comprobación de paridad, 184-185

comprobación de redundancia cíclica (CRC, *Cyclic Redundancy Check*), 185-191
detección y corrección de errores, 12
diafonía, 82, 824
diafonía cercana al extremo, y sistemas de cableado de par trenzado, 102
dificultades en la transmisión, 96
atenuación, 78-80
distorsión de retardo, 80
ruido, 80-83
difracción, 456
difusión, 595, 824
difusión de radio, 117
aplicaciones, 117
características de transmisión, 117
descripción física, 116-117
difusión directa vía satélite (DBS, *Direct Broadcast Satellite*), 115
digitalización, 157
diodo de inyección láser (ILD, *Injection Laser Diode*), 108
diodo emisor de luz (LED, *Light-Emitting Diode*), 108
dirección de difusión, 824
dirección de multidifusión, 824
dirección de subred de destino, cabecera del paquete, 44
dirección del computador de destino, 27
dirección multidestino de todos los computadores, 641
direccionamiento, 12, 216, 593-595
direcciones del punto de acceso a la red, 594
direcciones IP, 611-614
clases de redes, 611-612
máscaras de subred, 612-614
subredes, 612-614
disciplina de diálogo, capa de sesión, 39
disparidad, 548
dispersión, 109, 456, 824
distancia de Hamming, 193
distorsión de retardo, 80, 825
distribución de claves, cifrado simétrico, 733-735
centro de distribución de claves, 734
clave de sesión, 734
clave permanente, 734
módulo de servicio de seguridad (SSM, S*ecurity Service Module*), 734
y distribución de clave pública, 735
diversidad, 459
diversidad en frecuencias, 459
diversidad espacial, 459
división de celdas, 449-450
DM, *veáse* modulación delta (DM),
DMT, *véase* monotono discreto (DMT)
dominio de la frecuencia, 59, 62-66
ancho de banda absoluto, 65
ancho de banda efectivo, 65
componente continua, 65
espectro, 65
frecuencia fundamental, 63, 809
representaciones, 64
dos sentidos alternos, 197
dos sentidos simultáneos, 197
DS, *véase* servicios diferenciados (DS)
DSSS, *véase* espectro expandido de secuencia directa (DSSS)
DTE, *véase* equipo terminal de datos (DTE)

E

EBCDIC, 179
ecualización adaptativa, 459
efectos de la propagación de radio móvil, 454-456
desvanecimiento, 454
modelo de Okumura/Hata, 455
potencia de la señal, 454
eficiencia del ancho de banda, 153
EIA-568 (estándar de cableado de telecomunicaciones para edificios comerciales), 101
el mundo de las redes, 3
elemento de señal, 825
encaminador, 597-598, 825
encaminadores, 657-658
encaminamiento, 12, 604-605, 825
en redes conmutadas, 379-405
en redes de conmutación de circuitos, 380-382
encaminamiento alternativo, 381
en redes de conmutación de paquetes, 382-396
algoritmos de encaminamiento de primera generación, 392-393
algoritmos de encaminamiento de segunda generación, 393-394
algoritmos de encaminamiento de tercera generación, 394-396
características, 382-383
criterio de rendimiento, 383-384
ejemplos, 391-396
estrategias de encaminamiento, 386-391
fuente de la información de red y tiempo de actualización, 385-386
instante de decisión, 384-385
inundación, 387-389
lugar de decisión, 384-385
interconexión de redes no orientada a conexión, 604-605
lugar de decisión, 384-385
encaminamiento adaptable, 390-391
encaminamiento aleatorio, 389
encaminamiento en el origen, 501
encaminamiento estático, 386-387, 500-502
encaminamiento por estado de enlace, 644

encaminamiento por vector camino, 645
encaminamiento por vector distancia, 644
encapsulado, 589, 825
encapsulado de la carga útil de seguridad, 758-759
enlace de ida de IS-95, 464-467
  canal de localización, 465
  canal de sincronización, 465
  canal de tráfico, 466
  canal piloto, 465
  parámetros del canal, 465
  transmisión, 466
enlace de retorno de IS-95, 467-470
  parámetros del canal, 468
  transmisión, 469
enlace directo, 59
enlaces de redes (sitio web), 46
enlaces útiles sobre ATM, 376
enmascaramiento, 726
Equipo de Respuesta a Emergencias en Computadores (CERT, *Computer Emergency Response Team*), 754
equipo terminación de red, 825
equipo terminación de red (NT, *Network-Terminating Equipment*), 207
equipo terminación del circuito de datos (DCE, *Data Circuit-Terminating Equipment*), 199, 200, 203-204, 825
equipo Terminal (TE, *Terminal Equipment*), 207
equipo terminal de datos (DTE, *Data Terminal Equipment*), 199, 200, 204, 825
error de delimitación de trama, 181
espaciado entre canales en WDM de ITU, 258
especificación de gestión de tráfico, 424
especificaciones de IEEE 802.3 a 10 Mbps, 522-523
  alternativas definidas, 523
    10BASE2, 523
    10BASE5, 523
    10BASE-F, 523
    10BASE-T, 523
especificaciones de IEEE 802.3 a 100 Mbps (Fast Ethernet), 523-525
  100BASE-T4, 525-526
  100BASE-X, 525
  configuraciones mixtas, 526
  funcionamiento *full-duplex*, 526
  medios alternativos en la capa física, 525
  opciones, 524
espectro, 65, 825
espectro acústico para voz/música, 70
espectro de una señal, 137-138
espectro expandido, 285-305
  acceso múltiple por división de código, 286, 297-300
    para espectro expandido de secuencia directa, 299-300
    principios básicos, 297-299
  concepto, 286-287
espectro expandido de secuencia directa (DSSS, *Direct Sequence Spread Spectrum*), 286, 292-296
  acceso múltiple por división de código, 297-300
  consideraciones de rendimiento, 294-296
  usando BPSK, 293-294
  usando FSK múltiple (MFSK), 293-294
espectro expandido por salto de frecuencias rápido, 291
espectro expandido por salto en frecuencia, 286
  aproximación básica, 288-290
  cuestiones de rendimiento, 292
  uso de FSK múltiple (MFSK), 290-292
espectro expandido por salto en frecuencias lento, 291
espera exponencial binaria, 521, 697
esquema bipolar-AMI, 141
esquemas de reserva, 417
estación base, 447
estaciones, 311, 312
estado desocupado, 180
estado temporal, 664
estándar de cifrado avanzado (AES, *Advanced Encryption Standar*), 726, 729-732
estándar de cifrado de datos (DES, *Data Encryption Standard*), 728-729, 804
estándares, 4-6
estándares de portadoras TDM norteamericanas, 263
estándares internacionales de portadoras TDM, 263
estimación suavizada del tiempo de ida y vuelta, 708
estrella, 825
estructura, 536
estudiante de computación (williamstallings.com/StudentSupport.html), 3
Ethernet, 40, 516-530
  control de acceso al medio en IEEE 802.3, 516-523
    ALOHA, 516-517
    CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*, acceso multiple con detección de portadora y detección de colisiones), 519-521
    precursores, 516-519
    trama MAC, 522
  especificaciones de IEEE 802.3 a 10 Mbps, 522-523
    10BASE2, 523
    10BASE5, 523
    10BASE-F, 523
    10BASE-T, 523
    especificaciones del medio en 10BASE-T, 520
  especificaciones de IEEE 802.3 a 100 Mbps (*Fast Ethernet*), 523-526
    100BASE-T4, 525-526
    100BASE-X, 525
    configuración mixta, 526

medios alternativos para la capa física, 525
opciones, 524
operación *full-duplex*, 526
Ethernet a10 Gbps, 529-530
10GBASE-E, 530
10GBASE-L, 530
10GBASE-LX4, 530
10GBASE-S, 530
opciones de capa física, 529-530
opciones de velocidad y distancia, 530
Gigabit Ethernet, 526-529
capa de acceso al medio, 527-528
capa física, 528-529
Extended Binary Coded Decimal Interchange Code (EBCDIC), 179
extensiones multipropósito de correo electrónico (MIME), *véase* MIME (*Multipurpose Internet Mail Extension*,)

F

fase, 60, 825
FCS, *véase* secuencia de comprobación de trama (FCS)
FDM, *véase* multiplexación por división de frecuencia (FDM)
fibra óptica, 59, 105-109, 488, 825
aplicaciones, 105-107
características de transmisión,
cubierta, 105
descripción física, 105
propagación monomodo, 108
propagación multimodal de índice discreto, 107
propagación multimodo de índice gradual, 108
reflexión total interna, 107
revestimiento, 105
utilización de frecuencias para aplicaciones de fibra, 108
firma digital, 744-745, 825
FM, *véase* modulación de frecuencia (FM)
foco, 110
formateo de mensajes, 13
formato de trama MAC, 496-497
formato de transmisión DS-1, 263
formatos de codificación de datos digitales mediante señales digitales, 137
formatos de codificación digital de señales, 137-138
definición, 137
fórmula de la capacidad de Shannon, 84-86
foro ADSL, 280
foro ATM, 5, 376, 424, 430
Foro de interoperabilidad de SONET, 280
Foro de Retransmisión de Tramas, 346
Foro sobre IPv6, 628
frecuencia, 60, 825
frecuencia central, 68
frecuencia fundamental, 63, 809
frecuencias de microondas, 109
FSK multinivel (MFSK), 153
FSK múltiple (MFSK), 148, 290
FSK, *véase* modulación por desplazamiento de frecuencia (FSK)
FTP, *véase* protocolo de transferencia de ficheros (FTP)
fuente, modelo de comunicaciones, 11
función de dispersión, 825
función de dispersión segura SHA-1, 740-742
funcionamiento *full-duplex*, 526
funciones de dispersión seguras, 739-740
función de dispersión segura SHA-1, 740-742
requisitos, 740

G

ganancia, antenas, 110-111
ganancia de codificación, 196
generación de señal, 12
generatriz, 110
gestión de memorias temporales, 438
gestión de red, 13, 794-805
gestión de tráfico, 416-418
calidad de servicio (QoS, *Quality of Service*), 417
imparcialidad, 417
reservas, 417-418
Gestión de tráfico GFR en ATM, 436-439
contrato de tráfico GFR, 436-439
definición de adecuación GFR, 438-439
etiquetado, 438
gestión de memorias temporales, 438
mecanismo de comprobación de elegibilidad QoS, 439
planificación, 438
política, 438
trama adecuada pero inelegible, 439
trama adecuada y elegible, 439
trama no adecuada, 439
gestión del enlace, 216
gestión del intercambio, 12
gestión del temporizador de retransmisión:
algoritmo de Karn, 713-714
arranque lento, 714-715
decaimiento exponencial de RTO, 713
estimación de la variación del RTT, 709-714
modificación dinámica del tamaño de ventana en caso de congestión, 715-716
promedio exponencial, 708-709
Gigabit Ethernet, 526-529
1000BASE-CX, 528
1000BASE-LX, 528

1000BASE-SX, 528
1000BASE-T, 528
capa de acceso al medio, 527-528
capa física, 528-529
extensión de portadora, 527
ráfaga de tramas, 528
glosario, 821-830
Grupo de Desarrollo de CDMA, 474
Grupo de Trabajo de MGC, 346
Grupo de Trabajo de Servicios Diferenciados, 676
Grupo de Trabajo de Servicios Integrados (*Integrated Services Working Group*), 676
Grupo de trabajo OSPF, 676
Grupo de Trabajo RSVP, 676
grupo de trabajo sobre la red inalámbrica IEEE 802.11, 582
grupos de código, 543-545
grupos de noticias USENET, 4
grupos de potencia, y redes de alta velocidad, 515
grupos de servidores centralizados, y LAN de alta velocidad, 515
guía del lector, 1-5
esquema del libro, 2
estándares, 4-5
recursos en Internet/web, 2-4

H

haz IR dirigido, 565
HDLC *véase* control de enlace de datos de alto nivel (HDLC)

I

IAB, *véase* Junta de Arquitectura de Internet (IAB)
identificador de camino virtual (VPI, *Virtual Path Identifier*), 357, 373
identificador de canal virtual (VCI, *Virtual Channel Identifier*), 357, 373
identificador de conexión del enlace de datos (DLCI, *Data Link Connection Identifier*), 344, 595
identificador de transferencia (TID, *Transfer Identifier*), 49
identificadores de conexión, 578
IEEE 802, 5
IEEE 802.11, 567-572
arquitectura, 567-572
de protocolos, 574
capa física, 579-581
capa física original, 580
espectro expandido de secuencia directa, 580
espectro expandido por salto de frecuencia, 580
esquema infrarrojo, 580
IEEE 802.11a, 581
IEEE 802.11b, 581
IEEE 802.11g, 581
conjunto extendido de servicios (ESS, *Extended Service Set*), 569
control de acceso al medio (MAC, *Medium Access Control*), 570
control de acceso, 573-577
entrega de datos fiable, 572-573
función de coordinación distribuida (DFC, *Distributed Coordination Function*), 573-579
función de coordinación puntual, 577
trama MAC, 577-578
tramas de control, 578-579
tramas de datos, 579
tramas de gestión, 579
servicio de distribución, 570
servicio de integración, 570
servicios, 569-572
servicios de acceso y privacidad, 571-572
servicios relacionados con la asociación, 570-571
terminología, 568
IEEE *Communications Society*, 3
IETF, 3
IGMP, *véase* protocol de gestión de grupos en Internet (IGMP)
ILD, *véase* diodo de inyección láser (ILD)
IMT-TC, 471
incorporación de confirmación (*piggybacking*), 222, 825
indicador de la subcapa de convergencia (CSI, *Convergente SublayerIndicator*), 371
índice de modulación, 164
índice de refracción, 121
información de control del protocolo, 826
infrarrojo, 117
Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, *Institute of Electrical and Electronics Engineers*), 5
Instituto Europeo de Estándares de Telecomunicaciones (ETSI, *European Telecommunications Standards Institute*), 471
Instituto Nacional de Estándares y Tecnología (NIST, *National Institute of Standards and Technology*), 729
integración a gran escala (LSI, *Large ScaleIntegration*), 76
integración y selección del método de transmisión de datos, 78
integridad de los datos, y selección del método de transmisión, 77
interconexión de redes:
aproximaciones a la arquitectura, 599-600
arquitectura de servicios integrados (ISA, *Integrated Services Architecture*), 654-665

aproximación, 657-658
componentes, 658-659
disciplina de cola, 662-663
funciones de congestión, 658
protocolo de reserva de recursos (RSVP, *Resource Reservation Protocol*), 663-665
tráfico de internet, 654-657
tráfico elástico, 655-656
tráfico inelástico, 656-657
funcionamiento, 599-600
funcionamiento no orientada a conexión, 600
funcionamiento orientada a conexión, 599-600
interconexión de redes no orientada a conexión, 600-608
control de errores, 608
control de flujo, 608
cuestiones de diseño, 603-608
encaminamiento, 604-605
funcionamiento, 601-603
segmentación y reensamblado, 605-607
tiempo de vida del datagrama, 605
multidifusión, 633-642
aplicaciones, 633
estrategia de unidifusión múltiple, 634
estrategias de multidifusión, 634
protocolo de gestión de grupos en internet (IGMP, *Internet Group Management Protocol*), 638-642
requisitos, 635-637
tráfico generado, 631-678
protocolos de encaminamiento, 642.654
algoritmo de encaminamiento, 642
aproximaciones al encaminamiento, 644-645
encaminamiento por estado del enlace, 644
encaminamiento por vector camino, 644
encaminamiento por vector distancia, 644
información de encaminamiento, 642
protocolo de encaminador exterior (ERP, *Exterior Router Protocol*), 643
protocolo de pasarela fronteriza (BGP, *Border Gateway Protocol*), 645-651
protocolo del primer camino más corto disponible (OSPF, *Open Shortest Path First*), 651-654
protocolo interior de encaminador (IRP, *Interior Router Protocol*), 642
sistemas autónomos, 642-654
protocolos de transporte:
control de congestión en TCP, 707-716
mecanismos de los protocolos de transporte orientados a conexión, 680-699
TCP, 699-707
UDP, 716-717
requisitos, 598-599
servicios diferenciados (DS, *Differentiated Services*), comportamiento salto a salto, 672-674
configuración, 670-672
funcionamiento, 670-672
octeto, 668-670
servicios, 666-668
terminología, 597
interfaces, 198-209
características de procedimiento, 199
características eléctricas, 199
características funcionales, 199
características mecánicas, 199
circuitos de intercambio, 199
equipo terminación del circuito de datos (DCE, *Data Circuit-Terminating Equipment*), 199
equipo terminal de datos (DTE, *Data Terminal Equipment*), 199
interfaz física RDSI, 206-209
V.24/EIA-232-F, 200-206
interfaz, 12, 178
interfaz de programación de aplicaciones (API, *Application Programming Interface*), 814
interfaz física de RDSI, 206-209
conexión física, 207
especificación eléctrica, 208-209
interfaz socket de Berkeley, 814
interfaz usuario-red (UNI, *User-to-Network Interface*), 424-425
interferencia, 96
interferencia de señales e inmunidad al ruido, 139
interferencia intersimbólica (ISI, *Intersyimbol Intererence*), 457
interferencia multitrayectoria, 125-126
Internet, 597
intranet, 597
inundación, 387-389
IP, *véase* protocolo Internet (IP)
IPSec, 756-758
ámbito, 755
aplicaciones, 754-755
asociaciones de seguridad (SA, *Security Associations*), 755-756
cabecera de autenticación, 756-758
encapsulado de la carga útil de seguridad, 758-759
IPv6, 617-627
cabecera de encaminamiento, 626-627
cabecera de fragmentación, 626
cabecera de opciones salto a salto, 624-626
Direcciones, 623-624
Ipng (IP de nueva generación), 618-620
IS, *véase* sistema intermedio (IS)
ISA, *véase* arquitectura de servicios integrados (ISA)
ISO, *véase* Organización Internacional para la Estandarización
ITU-T (ITU, sector de telecomunicaciones), 5, 59

J

jerarquía digital síncrona (SDH, *Synchronous Digital Hierarchy*), 265, 350
julio (J), 81
Junta de Arquitectura de Internet (IAB, *Internet Architecture Board*), 40, 754

K

kelvin (K), 81

L

Laboratorio de Interoperabilidad, 540
Lamarr, Hedy, 286
LAN de alta velocidad, 513-555
  anillo de paso de testigo, 530-534
    control de acceso al medio (MAC, *Medium Access Control*), 532-534
    dedicado (DTR, *Dedicated Token Ring*), 534
    definición, 530
    funcionamiento del anillo, 530-531
    opciones de medios de transmisión en IEEE 802.5, 534
    principales desventajas, 534
    repetidores, 531
  características, 515
  cuestiones de rendimiento, 548-555
    modelos de rendimiento sencillos para paso de testigo y CSMA/CD, 552-555
    retardo de propagación / velocidad de transmisión, 549-551
  Ethernet, 516-530
    control de acceso al medio en IEEE 802.3, 516-522
    especificaciones de IEEE 802.3 a 10 Mbps, 522-523
    especificaciones de IEEE 802.3 a 100 Mbps (*Fast Ethernet*), 523-525
    Ethernet a 10 Gbps, 529-530
    Gigabit Ethernet, 526-529
  requisitos, 515
  surgimiento, 515-516
LAN, *véase* redes de área local (LAN)
LAN de espectro expandido, 565-566
  configuración, 565-566
  cuestiones de transmisión, 566
LAN de microondas de banda estrecha, 566-567
  RF de banda estrecha con licencia, 567
  RF de banda estrecha sin licencia, 567
LAN en bus, 486
  medios alternativos, 488
LAN inalámbricas, 557-583
  aplicaciones, 558-561
    acceso nómada, 561
    extensión de LAN, 559
    interconexión entre edificios, 561
    redes ad hoc, 561
  IEEE 802.11, 567-572
    arquitectura, 567-569
    capa física, 579-581
    conjunto extendido de servicios (ESS, *Extended Service Set*), 569
    control de acceso al medio (MAC, *Medium Access Control*), 572-579
    servicio de distribución, 570
    servicio de integración, 570
    servicios, 569-572
    servicios de acceso y privacidad, 571-572
    servicios relacionados con la asociación, 570-571
    terminología, 568
  requisitos, 561-563
  tecnología, 563-567
LAN infrarroja, 563-565
  configuración de difusión, 565
  configuración omnidireccional, 565
  haz IR dirigido, 565
  técnicas de transmisión, 565
  ventajas/desventajas, 564-565
LAPF (*Link Access Procedure for Frame Mode Bearer Services*, procedimiento de acceso al enlace para servicios en modo trama), 343
ley de Carson, 169
línea de abonado digital asimétrica (ADSL), 156, 275-277
  diseño, 275-277
  monotono discreto (DMT, *Discrete Monotone*), 277.278
línea de abonado, red pública de telecomunicaciones, 314
línea digital de abonado (DSL, *Digital Suscriber Line*), 18
línea digital de abonado de alta velocidad (HDSL, *high data rate digital suscriber line*), 278
línea digital de abonado de muy alta velocidad (VDSL, *Very High Data Rate Digital Suscriber Line*), 279
línea digital de abonado de una sola línea (SDSL, *Single Line Digital Suscriber Line*), 279
línea visual óptica y de radio, 59, 105-109, 488, 823
LLC, *véase* control de enlace lógico (LLC)
lógica digital, 179-191
longitud de onda, 62

M

MAC, *véase* control de acceso al medio (MAC)
macroceldas, parámetros típicos, 450
marcado de celdas, 435

McDonald, Chris, 818
mecanismos de acondicionamiento de tráfico, 670-671
  bloque de descarte de paquetes, 671
  clasificador, 671
  conformador, 671
  marcador, 671
  monitor, 671
mecanismos de compensación de errores, 459
mecanismos de los protocolos de transporte orientados a conexión:
  servicio de red de entrega ordenada fiable, 681-689
  servicio de red no fiable, 689-699
medio de transmisión guiado, 59, 96, 97-109, 98
  cable coaxial, 104-105
  par trenzado, 99-103
medio de transmisión no guiado, 59, 96
medios de transmisión, 95-131
  definición, 96
  fibra óptica, 105-109
  propagación inalámbrica, 117-122
  transmisión visual, 122-126
mensaje consulta de pertenencia a grupo (*membership query*), 638
  campos, 639
  consulta de grupo específico, 639
  consulta de grupo y fuente específicos, 639
  consulta general, 638
mensaje de informe de pertenencia a grupo (*membership report*), 640
  campo de grupo de registros, 640-641
  campos, 640
mensajes de respuesta, 790-793
mensajes de solicitud, 786-790
métodos de codificación de bloques, 546-547
microceldas, 450
  parámetros típicos, 450
microondas, 112-113
  de banda estrecha, 566-567
  de satélite, 113-116
  terrestres, 112-113
microondas de corto alcance, 112
microondas de satélite, 113-116
  aplicaciones, 114-116
  características de transmisión, 116
  descripción física, 113-114
microondas terrestres, 112-113
  aplicaciones, 112
  características de transmisión, 112-113
  descripción física, 112
MIME (*Multipurpose Internet Mail Extension*, extensiones multipropósito de correo electrónico), 764, 772-780
  campos de cabecera de mensaje, 773
  definición, 772
  esquemas de codificación de transferencia, 777780
    binaria, 777
    codificación de transferencia base64, 778
    representación general de 7 bits, 777
    representación general de 8 bits, 777
    representación *quoted-printable* (imprimible textualmente), 777
    x-token, 777
  tipo de aplicación, 776
    subtipo *application*/*octet-stream* (aplicación/secuencia de octetos), 776
    subtipo *application*/*Postscript* (aplicación/postscript), 777
    subtipo *message*/*external-body* (mensaje/cuerpo-externo): 776
    subtipo *message*/*partial* (mensaje/parcial): 775
    subtipo *message*/*rfc*822 (mensaje/rfc822), 775
    subtipo *multipart*/*alternative* (multiparte/alternativo), 775
    subtipo *multipart*/*digest* (multiparte/resumen), 775
    subtipo *multipart*/*mixed* (multiparte/mixto), 775
    subtipo *multipart*/*parallel* (multiparte/paralelo), 775
    tipo audio, 776
    tipo *image* (imagen), 776
    tipo *message* (mensaje), 775
    tipo *multipart* (multiparte), 775
    tipo *text* (texto), 776
    tipo *video* (vídeo), 776
  tipos de contenido, 773-777
  visión general, 772-771
MIME, subtipo *Application*/*octet-stream*, 776
MIME, subtipo *Application*/*Postscript*, 777
MIME, tipo *Application* (aplicación), 776
MLT-3, 545-546
modelo de comunicaciones, 10-13
modelo de control de acceso basado en vistas (VACM, *View-Based Access Control Model*), 804
modelo de referencia IEEE 802, 490-499
modelo de referencia para la interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*), 22, 29-39, 826
  capa de acceso a la red, 25
  capa de aplicación, 31, 40
  capa de control de enlace de datos, 31, 37
  capa de presentación, 31, 39
  capa de sesión, 31-32, 38
  capa de transporte, 121-122
  capa física, 31, 36-37, 490
  capas, 36-39
    definición, 31
    justificación, 32
    principios usados en la definición, 30
  marco de trabajo OSI, estandarización, 32-35
    definición de servicios, 34

direccionamiento, 34
especificación de protocolos, 33
modelo, 29-32
primitivas de servicio y parámetros, 35-36
tipos, 35
modelo de seguridad basado en el usuario (USM, *User-Based security*), 804
módem (modulador/demodulador), 75, 826
módem asimétrico de línea privada, 203
módem de cable, 274
módem de distancia limitada, 204
módem nulo, ejemplo, 207
módem telefónico, 18-19
modo de direccionamiento, 595
modo de transferencia asíncrono (ATM, *Asynchronous Transfer Mode*), 16, 349-378, 632, 826
arquitectura de protocolos, celdas, 350-351
caminos virtuales:
características, 354-355
mecanismos de control, 352
terminología, 354
ventajas, 352
canal virtual:
calidad de servicio, 354
características, 354-355
conexiones de camino virtual conmutadas/semipermanentes, 355
integridad de la secuencia de celdas, 355
negociación de los parámetros de tráfico y supervisión de uso, 355
restricción de identificador en un VPC, 355
usos de la conexión, 353.-354
capa de adaptación ATM (AAL, *ATM Adaptation Layer*), 350-351, 368-375
AAL tipo 1, 371-372
AAL tipo 2 y 3/4, 372-373
AAL tipo 5, 373-375
emulación de circuitos, 369
emulación LAN (LANE), 369
encapsulado multiprotocolo sobre ATM (MPOA), 369
IP sobre ATM, 369
servicios AAL, 368-369
servicios generales de datos, 369
voz y vídeo a VBR, 369
categorías de servicios, 365-368
celdas, 365-361
campo de control de errores de cabecera, 358
campo de control de flujo genérico (GFC), 356-357, 359
control de errores de cabecera, 360-361
control de flujo genérico (GFC, *Generic Flow Control*), 358-359
formato de la cabecera, 356-358
identificador de camino virtual (VPI, *Virtual Path Identifier*), 357
identificador de canal virtual (VCP, *Virtual Channel Identifier*),
prioridad de pérdida de celdas (CLP, *Cell Loss Priority*), 358
tipo de carga útil (PT, *Payload Type*), 357
conexiones de canal virtual (VCC,V*irtual Channel Connection*), 351
conexiones lógicas, 351-356
definición, 350
gestión de tráfico/control de congestión, 424-436
adaptación del tráfico, 436
contribución de la red a la variación del retardo de celdas, 427-428
control de admisión de conexión, 432
control de parámetros de uso, 434-435
controles a largo plazo, 429
duración de la conexión, 429-430
efectos de la latencia/velocidad, 425-426
gestión de recursos usando caminos virtuales, 430-432
objetivos de, 429
rechazo selectivo de celdas, 435-436
requisitos, 424-425
técnicas, 430-436
tiempo de inserción de celda, 429-430
tiempo de propagación de ida y vuelta, 429
variación del retardo de celdas, 426-429
variación del retardo de celdas en la UNI, 428-429
gestión de tráfico GFR en ATM, 436-439
contrato de tráfico GFR, 438
definición de adecuación GFR, 438-439
etiquetado, 438
gestión de memorias temporales, 438
mecanismo de comprobación de elegibilidad QoS, 439
planificación, 438
política de uso, 438
trama adecuada pero inelegible, 439
trama adecuada y elegible, 439
trama no adecuada, 439
plano de control, 351
plano de gestión, 351
plano de usuario, 351
señalización de control, 355-356
canal de metaseñalización, 356
canal virtual de señalización usuario-red, 356
canal virtual de señalización usuario-usuario, 356
VCC semipermanente, 355
servicios en no tiempo real, 366-368
velocidad de tramas garantizada (GFR, *Guaranteed Frame Rate*), 367-368
velocidad disponible (ABR, *Available Bit Rate*), 367

velocidad no especificada (UBR, *Unspecified Bit Rate*), 367
velocidad variable en no tiempo real (nrt-VBR, *non real time Variable Bit Rate*), 366
servicios en tiempo real, 365-366
servicios en no tiempo real, 366-368
velocidad constante (CBR, *Constant Bit Rate*), 366
velocidad variable en tiempo real (rt-VBR, *real time Variable Bit Rate*), 366
transmisión de celdas, 362-365
capa física basada en celdas, 362-364
capa física basada en SDH, 364-365
modo no asociado, 324
modos de operación de DES (*National Bureau of Standards*), 737
modulación, 135, 164, 826
modulación angular, 166-169
modulación de amplitud (AM, *Amplitude Modulation*), 134, 163-166, 826
modulación de amplitud en cuadratura (QAM, *Quadrature Amplitude Modulation*), 156, 237
modulación de fase (PM, *Phase Modulation*), 134, 826
modulación de frecuencia (FM, *Frecuency Modulation*), 134, 169, 826
modulación delta (DM, *Delta Modulation*), 160-162
ejemplo, 161
Modulación en doble banda lateral con portadora (DSBTC, *Double Sideband Transmitted Carrier*), 164-166
modulación por amplitud de pulso (PAM, *Pulse Amplitude Modulation*), 158
modulación por código de pulso (PCM, *Pulse Code Modulation*), 157, 162-163, 264, 826
modulación por desplazamiento de amplitud (ASK, *Amplitude Shift Keying*), 134, 146, 147, 155-157, 826
modulación por desplazamiento de fase (PSK, *Phase-Shift Keying*), 134, 146, 149-153, 199, 826
PSK de cuatro niveles, 150-152
PSK de dos niveles, 149-150
PSK multinivel, 152-153
modulación por desplazamiento de fase binaria (BPSK, *Binary PSK*), 288
modulación por desplazamiento de fase en cuadratura (QPSK, *Quadrature Phase Shift Keying*), 150-152, 156
modulación por desplazamiento de frecuencia (FSK, *Frecuency Shift Keying*), 147-149, 288, 826
módulo de transferencia de archivos, 23
monodifusión e IPv6, 624
monotono discreto (DMT, *Discrete Monotone*), 275, 277-278
multidifusión, 595, 633-664
aplicaciones, 633
e IPv6, 624
estrategia de unidifusión múltiple, 634
estrategias de multidifusión, 634
protocolo de gestión de grupos en internet (IGMP, *Internet Group Management Protocol*), 638-642
requisitos, 635-637
tráfico generado, 635
multiplexación, 11, 249-283, 595-596, 827
definición, 250
línea de abonado digital asimétrica (ADSL, *AsymmetricDigital Suscriber Line*),
diseño, 275-277
monotono discreto (DMT, *Discrete Monotone*), 277-278
multiplexación estadística, conexiones de camino virtual (VPC, *Virtual Path Connections*), 430
multiplexación por división en el tiempo (TDM, *Time Division Multiplexing*), 163, 250-251, 312
multiplexación por división en el tiempo estadística, 250, 826
características, 268-270
módem de cable, 274
rendimiento, 270-274
multiplexación por división en el tiempo síncrona, 250, 826
características, 258-260
control del enlace en TDM, 260-263
sistemas de portadora digital, 263-264
SONET/SDH, 265-267
multiplexación por división en frecuencia (FDM, *Frecuency Division Multiplexing*), 104, 162, 250, 251-259, 276, 312, 313, 826
características, 251-256
multiplexación por división en la longitud de onda (WDM, *Wavelength Division Multiplexing*), 257-258
sistemas con portadora analógica, 256-257
multiplexación por división en la longitud de onda densa (DWDM, *Dense WDM*), 257
xDSL, 278-279
línea digital de abonado de alta velocidad (HDSL, *High Data Rate Digital Suscriber Line*), 278
línea digital de abonado de muy alta velocidad (VDSL, *Very High Data Rate Digital Suscriber Line*), 279
línea digital de abonado de una sola línea (SDSL, *Single Line Digital Suscriber Line*), 279
y comunicaciones de datos, 250-251
multipunto, 827

N

nivel de direccionamiento, 593
no retorno a cero (NRZ, *Nonreturn to Zero*), 74, 139-140, 141

no retorno a cero, unos invertidos (NRZI, *Nonreturn to Zero*, *Invert on Ones*), 139
no retorno a nivel cero (NRZ-L, *Nonreturn to Zero-Level*), 139, 200
nodos, 536
nodos fronterizos, 15
notación de sintaxis abstracta 1, 827
notificación explícita de congestión hacia atrás (BECN, *Backward Explicit Congestion Notification*), 423-424
notificación explícita de congestión hacia delante (FECN, *Forward Explicit Congestion Notification*), 423-424
NRZ, *véase* no retorno a cero (NRZ)
NRZ-L, *véase* no retorno a nivel cero (NRZ-L)
número de saltos, 827
número de secuencia (SN, *Secuence Number*), 371
  cabecera de PDU de transporte, 27
  cabecera TCP, 43

O

octeto, 827
onda periódica, 827
onda seno, 60
onda sinusoidal genérica, 61
opciones de medios de transmisión en IEEE 802.5, 534
OQPSK, *véase* QPSK desplazada (OQPSK)
organización de las redes celulares, 446-451
Organización Internacional de Estandarización (ISO, *International Organization for Standarization*), 5, 29
Organización Nacional de Estandarización, 3
OSI, *véase* interconexión de sistemas abiertos (OSI)

P

página de herramientas, 818
página de información sobre IPv6, 628
página de recursos sobre tecnología de telecomunicaciones, 4
página web de SONET, 280
palabra código, 192-195
paquete de obstrucción, 414-415
paquete de ralentización del emisor de ICMP, 414
paquetes, 15, 44, 410, 827
par trenzado, 59, 98-103, 488, 827
  aplicaciones, 99
  características de transmisión, 99-100
  descripción física, 99
  tipos y clases, 102
  UTP de tipo 3 y tipo 5, 102
par trenzado apantallado (STP, *Shielded Twisted Pair*), 100-101
par trenzado no apantallado (UTP, *Unshielded Twisted Pair*), 100-101
paraboloide, 110
parada y espera, 827
pasarela, 783-784
pasarela de medios (MG, *Media Gateway*), 330
patrón de bits final, 181
patrón de bits inicial, 181
PBX, *véase* centralita privada (PBX)
PCM, *véase* modulación por código de pulso (PCM)
PDU, *véase* unidad de datos del protocolo (PDU)
PDU de acceso a la red, 27
PDU de transporte, 27
pérdidas en el espacio libre, 122-124
periodo, 60, 827
PHB de reenvío asegurado, 673-674
PHB de reenvío urgente, 672-673
plano de control, 327
  ATM, 351
plano de gestión:
  ATM, 351
plano de información, 327
PM, *véase* modulación de fase (PM)
polinomios, 188-189
política de tráfico, 436
portadora, 827
portadora común, 827
potencia, en el rendimiento de la red, definición, 412
potencia media de una señal de duración limitada, 810-812
primitiva de confirmación, 36
primitiva de indicación, 35
primitiva de respuesta, 35
primitiva de solicitud, 35
principios de los códigos de bloque, 193-197
prioridad de pérdida de celdas (CLP, *Cell Loss priority*), 358
privacidad, y selección del método de transmisión de datos, 78
programación de *sockets*, 814
propagación aérea de ondas, 120
propagación en línea visual, 120-122
  línea visual óptica y de radio, 121
  refracción, 120-121
propagación inalámbrica, 117-122
  propagación aérea de ondas, 120
  propagación en línea visual, 120-121
  propagación superficial, 119-120
propagación monomodal, 108
propagación multimodal de índice discreto, 107
propagación multimodo de índice gradual, 108
propagación multitrayectoria, efectos, 457-458

propagación superficial, 119-120
protocolo, 827
  definición, 23
protocolo 1 persistente, 518
protocolo de control de la transmisión (TCP)/protocolo Internet (IP), *véase* TCP/IP
protocolo de control de la transmisión (TCP, *Transmisión Control Protocol*), *véase* TCP
protocolo de datagrama de usuario, *véase* UDP
protocolo de encaminador exterior (ERP, *Exterior Router Protocol*), 643
protocolo de gestión de grupos en internet (IGMP, *Internet Group Management Protocol*), 638-642
  formato de mensaje, 638-642
    mensaje consulta de pertenencia a grupo (*membership query*), 638
    mensaje informe de pertenencia a grupo (*membership report*), 640
  funcionamiento, 641-642
  pertenencia a grupo en IPv6, 642
protocolo de información de encaminamiento (RIP, *Routing Information Protocol*), 644
protocolo de mensajes de control de internet (ICMP, *Internet Control Messages Protocol*), 614-617
  mensaje de destino inalcanzable, 616
  mensaje de eco/respuesta a eco, 617
  mensaje de marca de tiempo / respuesta de marca de tiempo, 617
  mensaje de ralentización del origen, 616
  mensaje de redirección, 616
  mensaje de tiempo excedido, 616
  mensajes de solicitud de la máscara de dirección/respuesta de máscara de dirección, 617
protocolo de pasarela fronteriza (BGP, *Border Gateway Protocol*), 645-651
  funciones, 645-647
  intercambio de información de encaminamiento, 650-651
  mensajes, 647-650
    atributo AS_Path, 648, 650
    campo de atributos del camino, 648
    campos, 647
    formatos, 648
    mensaje de notificación, 649
    mensaje Keepalive, 647
    mensajes de actualización, 647
protocolo de reserva de recursos (RSVP, *Resource Reservation Protocol*), 417, 663-665
  características, 665
  estado temporal, 664
  multidifusión, 664
  unidifusión, 664
protocolo de transferencia de archivos (FTP, *File Transfer Protocol*), 44, 655, 680
protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*), 780-794
  caché, 784
  campos de la cabecera general, 786
  elementos, 787
  entidades, 793-794
    campos de cabecera, 793-794
    cuerpo, 794
  mensajes, 784-786
    mensajes de solicitud simple y respuesta simple, 786
  mensajes de respuesta, 790-793
    campos de cabecera, 791-793
    códigos de estado, 790-791
  mensajes de solicitud, 786-790
    campos de cabecera de solicitud, 789-790
    métodos de solicitud, 788-789
  pasarela, 793
  representante, 782-783
  túnel, 784
  visión general, 780-784
protocolo de ventana deslizante:
  ejemplo, 222
  temporización, 244
protocolo del primer camino más corto disponible (OSPF, *Open Shortest Path First*), 644, 651-654
protocolo interior de encaminador (IRP, *Interior Router Protocol*), 626
protocolo internet (IP, *Internet Protocol*), 40, 599, 608-617
  direcciones IP, 611-614
    clases de redes, 611-612
    máscaras de subred, 612-614
    subredes, 612-614
  primitiva *Deliver*, 608
  primitiva *Send*, 608
  protocolo, 609-611
  protocolo de mensajes de control de internet (ICMP, *Internet Control Messages protocol*), 614-617
    mensaje de destino inalcanzable, 616
    mensaje de eco/respuesta a eco, 617
    mensaje de marca de tiempo/respuesta de marca de tiempo, 617
    mensaje de ralentización del origen, 616
    mensaje de redirección, 616
    mensaje de tiempo excedido, 616
    mensajes de solicitud de la máscara de dirección / respuesta de máscara de dirección, 617
  protocolo entre entidades IP, 609-611
  servicios, 608-609
protocolo *p*-persistente, 518
protocolo simple de gestión de red (SNMP, *Simple Network Management Protocol*), 42, 45, 655, 794-805
  arquitectura de protocolos de gestión de red, 797-798

sistemas de gestión de red, 795
versión 1 (SNMPv1), 795-798
agente de gestión, 796
base de datos de información de gestión (MIB, *Management Information Base*), 796
conceptos básicos, 795-797
estación de gestión, 795
papel de, 799
protocolo de gestión de red, 796
versión 2 (SNMPv2), 798-804
elementos, 799-801
estructura de información de gestión (SMI, *Structure of Management Information*), 801
funcionamiento del protocolo, 801-803
PDU *InformRequest*, 803
PDU *SNMPv2-Trap*, 803
versión 3 (SNMPv3), 804-805
protocolo simple de transferencia de correo electrónico (SMTP, *Simple Mail Transfer Protocol*), 44, 655, 680, 764-772
cierre de conexión, 771
comando DATA, 770
comando MAIL, 770
comando RCPT, 770
definición, 765
emisor SMTP, 766, 771
establecimiento de conexión, 768-769
funcionamiento básica del correo electrónico, 765-767
órdenes, 768
protocolo SMTP, 766
receptor SMTP, 766-767
respuestas SMTP, 767
RFC 822, 771
transferencia de correo, 769-771
visión general, 767-768
protocolo trivial para la transferencia de archivos (TFTP, *Trivial File Transfer Protocol*), 23, 49-52
definición 49,
errores/retardos, 51-52
paquetes, 49-50
paquete RRQ, 49
paquete WRQ, 50
semántica, 52
sintaxis, 52
temporización, 52
transferencia, visión general, 51
protocolos de control de enlace de datos, 215-248
control de errores, 216, 223-229
definición, 223
solicitud de repetición automática (ARQ, *Automatic Repeat Request*), 224-229
técnicas habituales, 224
trama dañada, 224
trama perdida, 223
control de flujo, 216, 217-223
control de flujo de parada y espera, 218-220
control de flujo de ventana deslizante, 220-223
definición, 217
control del enlace de datos de alto nivel (HDLC, *High-Level Data Link Control*), 229-236
características básicas, 229-230
estructura de trama, 230-233
funcionamiento, 223-226
definición, 216
protocolos de encaminamiento, 632, 644-654
algoritmo de encaminamiento, 642
aproximaciones al encaminamiento, 644-645
encaminamiento por estado del enlace, 644
encaminamiento por vector camino, 645
encaminamiento por vector distancia, 644
información de encaminamiento, 642
protocolo de encaminador exterior (ERP, *Exterior Router Protocol*), 643
protocolo de pasarela fronteriza (BGP, *Border Gateway Protocol*), 645-651
protocolo del primer camino más corto disponible (OSPF, *Open Shortest Path First*), 651-654
protocolo interior de encaminador (IRP, *Interior Router Protocol*), 642
sistemas autónomos, 642-644
protocolos de encaminamiento en internet, 632
protocolos de interconexión de redes, 587-630
cabecera IPv6, 620-623
campo cabecera siguiente, 621
campo clase de tráfico, 621
campo dirección de destino, 622
campo dirección origen, 621
campo etiqueta de flujo, 621, 622-623
campo límite de saltos, 621
campo longitud de la carga útil, 621
campo versión, 621
campos, 621
control de conexión, 590-591
control de errores, 592-593
control de flujo, 592
direccionamiento, 593-595
encapsulado, 589
entrega ordenada, 592
funciones básicas del protocolo, 588-596
interconexión de redes:
aproximaciones a la arquitectura, 599-600
funcionamiento no orientado a conexión, 599-600
funcionamiento orientado a conexión, 600
interconexión de redes no orientada a conexión, 600-608
principios, 597-600
requisitos, 598-599

interconexión de redes no orientada a conexión, 600-608
IPv6,
cabecera de encaminamiento, 626-627
cabecera de fragmentación, 626
cabecera de opciones salto a salto, 624-626
direcciones, 623-624
IPng (IP de nueva generación), 618-620
multiplexación, 595-596
protocolo internet (IP), 588, 598, 608-617
segmentación y reensamblado, 589-590
servicios de transmisión, 596
protocolos de red:
aplicaciones distribuidas, 763-806
correo electrónico, 764- 780
gestión de red, 794-805
MIME (*Multipurpose Internet Mail Extension*, extensiones multipropósito de correo electrónico), 764, 772-780
protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*), 780-794
protocolo simple de gestión de red (SNMP, *simple network management protocol*), 794-805
protocolo simple de transferencia de correo electrónico (SMTP, *Simple Mail Transfer Protocol*), 764-772
protocolos de interconexión de redes, 587-630
funciones básicas del protocolo, 588-596
interconexión de redes no orientada a conexión, 600-608
IPv6, 617-627
principios de interconexión de redes, 597-600
protocolo de Internet (IP, *Internet Protocol*), 588, 608-617
protocolos de transporte, 679-721
control de congestión en TCP, 707-716
mecanismos de los protocolos de transporte orientados a conexión, 680-699
servicio de red de entrega ordenada fiable, 681-689
servicio de red no fiable, 689-699
TCP, 699-707
UDP, 716-717
seguridad en red, 723-762
algoritmo de cifrado de clave pública RSA, 745-747
amenazas pasivas, 725-726
ataques activos, 726
ataques de denegación de servicio, 726
ataques pasivos, 725-726
autenticación de mensajes, 735-739
capa de *sockets* segura (SSL, *Secure Sockets Layer*), 724, 749-754
capa de transporte segura (TLS,*Transport Layer Security*), 724-749
cifrado, 724, 726-735
cifrado de clave pública, 724, 742-744
cifrado simétrico, 724
definición, 724
e integridad, 725
enmascaramiento, 726
firma digital, 744-745
funciones de dispersión seguras, 739-740
IPSec, 724
modificación de los mensajes, 726
repetición, 726
requisitos relacionados, 724-725
seguridad de la información, 724
seguridad de los computadores, 724
seguridad en IPv4 e IPv6, 754-759
tecnología subyacente, 724-725
y autenticación, 725
y confidencialidad, 725
y disponibilidad, 725
TCP, 699-707
establecimiento de conexión, 703-704
formato de cabecera, 699-703
mecanismos, 703-704
opciones de implementación de la política, 705-707
parámetros de servicio, 702
política de aceptación, 705-706
política de confirmación, 706-707
política de entrega, 705
política de envío, 705
política de retransmisión, 706
primitivas de respuesta del servicio, 701
primitivas de solicitud del servicio, 700
servicios, 699
terminación de conexión, 704
transferencia de datos, 704
UDP, 716-717
proveedor de servicios internet (ISP, *Internet Services Provider*), 18
Proyecto RSVP, 676
proyectos de investigación, 819
proyectos para la enseñanza de comunicaciones y redes de computadores, 817-819
asignaciones de lecturas/trabajos, 819
modelado de rendimiento, 818
proyectos de investigación, 819
proyectos de simulación, 817-818
simulador de red *cnet*, 817-818
PSD, *véase* densidad de potencia espectral (PSD)
pseudoternario, 141
PSK de cuatro niveles, 150-152
PSK de dos niveles, 149-150
PSK diferencial (DPSK), 150
PSK multinivel (MPSK), 153
PSK, *véase* modulación por desplazamiento de fase (PSK)
puentes, 497-504, 598, 827

algoritmo del árbol de expansión, 501, 503-504
aprendizaje de direcciones, 503
aproximación del árbol de expansión, 502-504
arquitectura de protocolos, 499-500
base de datos de retransmisión, 502
configuración del encaminamiento estático, desarrollo, 501-502
encaminamiento en el origen, 501
encaminamiento estático, 500-502
fiabilidad, 497
funciones, 498-499
geografía, 498
prestaciones, 497
seguridad, 497
puerto de destino, cabecera TCP, 43
puertos, 25
punto a punto, 59, 827
punto de acceso al servicio de red (NSAP, *Network Service Acess Point*), 34, 594
punto de señalización (SP, *Signaling Point*), 327
punto de transferencia de señal (STP, *Signal Transfer Point*), 328
punto raíz, 274
puntos de acceso al servicio (SAP, *Service Access Point*), 25, 42, 370, 594, 827

Q

QPSK desplazada (OQPSK, *offset QPSK*), 151

R

radio, 116-117
radioLAN, 567
ráfaga de errores, 182
ráfaga de tramas, Gigabit Ethernet, 528
RDSI de banda ancha (RDSI-BA), 827
receptor no preparado (RNR, *Receiver Not Ready*), 236
receptor RAKE, 463
receptores, 11, 97
recuperación, 13
capa de sesión, 39
recursos web/internet, 2-4
grupos de noticias de USENET, 4
rechazo selectivo (SREJ), 228
rechazo selectivo de celdas, 435
red de comunicaciones de datos, 14-17
redes de área amplia (WAN, *Wide Area Network*), 15-16
conmutación de circuitos, 15
conmutación de paquetes, 15
retransmisión de tramas, 16
redes de área local (LAN, *Local Area Network*), 17
redes de área metropolitana (MAN, *Metropolitan Area Network*), 17
redes inalámbricas, 17
red de comunicaciones por difusión, 828
red de datos pública, 828
red de valor añadido, 828
red digital de servicios integrados (RDSI), 828
red troncal local de alta velocidad, y LAN de alta velocidad, 513
redes celulares inalámbricas, 431-476
adición de nuevos canales, 449
analógicas de primera generación, 460-461
asignación de frecuencias, 460
canales de control de AMPS, 461
funcionamiento, 461
módulo de asignación numérica (NAM, *Numeric Assignment Module*), 461
analógicas de segunda generación, 461-470
acceso múltiple por división de código (CDMA, *Code Division Multiple Access*), 462-463
aspectos de diseño de CDMA móvil inalámbrico, 463-464
comparación con sistemas de primera generación, 462
enlace de ida en IS-95, 464-467
enlace de retorno en IS-95, 467-470
IS-95, 464
aumento de la capacidad, 449-451
central de conmutación de telecomunicaciones móviles (MTSO, *Mobile Telecommunications Switching Office*), 451-454, 461
aceptación de la llamada, 453
bloqueo de llamadas, 454
corte de llamadas, 454
inicialización de la unidad móvil, 452
localización, 452
llamada en curso, 454
llamada originada en un móvil, 452
llamadas a/desde usuarios fijos y móviles, 454
terminación de llamadas, 454
traspaso, 454
desvanecimiento, 456-459
corrección de errores hacia adelante, 459
desvanecimiento lento, 458
desvanecimiento plano, 458
desvanecimiento rápido, 458
desvanecimiento selectivo, 458
difracción, 453
dispersión, 456
diversidad, 459
diversidad en frecuencias, 459
diversidad espacial, 459
ecualización adaptativa, 459

mecanismos de compensación de errores, 459
propagación multitrayectoria, 456-457
reflexión, 456
tipos, 458-459
división de celdas, 449-450
efectos de propagación en radio móvil, 454-456
desvanecimiento, 454
modelo de Okumura/Hata, 455
potencia de la señal, 454
estación base, 447
funcionamiento, 451-454
macroceldas, parámetros típicos, 450
microceldas,
parámetros típicos, 450
organización de las redes celulares, 446-451
principios, 446-459
reutilización de frecuencias, 447-449
patrones de, 448
sectorización de celdas, 449-450
sistemas de tercera generación, 470-473
aspectos de diseño de CDMA, 472-473
capacidades, 470
interfaces alternativas, 471-472
uso de frecuencias prestadas, 449
redes de área amplia (WAN, W*ide Area Network*), 10, 15-17
congestión, 407-443
conmutación de circuitos, 15
conmutación de circuitos/conmutación de paquetes, 309-348
conmutación de paquetes, 15
encaminamiento en redes conmutadas, 379-405
modo de transferencia asíncrono (ATM, *Asynchronous Transfer Mode*), 349-378
redes celulares inalámbricas, 445-476
retransmisión de tramas, 15-16
redes de área local (LAN, *Local Area Network*), 10, 15, 17, 97, 477-583, 828, *véase también* LAN de alta velocidad; LAN infrarrojas y LAN inalámbricas
arquitectura de protocolos, 489-497
modelo de referencia IEE 802, 490-492
codificación digital de señales para, 543-548
4B/5B-NRZI, 543-545
8B10B, 548
8B6T, 546-548
MLT-3, 545-546
conmutadores, 504-509
concentrador raíz (HHUB), 505
concentradores, 504-505
concentradores intermedios (IHUB), 505
conmutador de almacenamiento y envío, 507
conmutador rápido, 507
conmutadores de capa 2, 505-507
conmutadores de capa 3, 508-509
control de acceso al medio (MAC, *Medium Access Control*), 491, 494-497
contención, 496
formato de trama MAC, 496-497
reserva, 496
rotación circular, 495-496
control del enlace lógico (LLC, *Logical Link Control*), 492-495
protocolos, 493-495
servicios, 492-493
elementos clave, 484
fundamentos, 480-484
LAN de computadores personales, 480-481
LAN troncales, 483-484
redes de almacenamiento, 481-483
redes de respaldo, 481-483
redes ofimáticas de alta velocidad, 483
LAN de alta velocidad, 514-555
LAN inalámbricas, 553-583
medio de transmisión, elección, 488-489
puentes, 497-504
algoritmo del árbol de expansión, 501, 503-504
aprendizaje de direcciones, 503
aproximación del árbol de expansión, 502-504
arquitectura de protocolos, 499-500
configuración del encaminamiento estático, desarrollo, 501-502
encaminamiento en el origen, 501
encaminamiento estático, 500-502
fiabilidad, 497
funciones, 498-499
geografía, 498
rendimiento, 497
retransmisión de tramas, 502
seguridad, 497-498
redes de área metropolitana (MAN, *Metropolitan Area Network*), 17
redes inalámbricas, 17
topologías, 480, 484-489
LAN en bus, 484-486
topología en anillo, 486-487
topología en árbol, 484-486
topología en estrella, 488
visión general, 479-512
redes de área metropolitana (MAN, *Metropolitan Area Network*), 17
redes de comunicaciones, 311, 828
redes de comunicaciones conmutadas, 299-300, 828
redes de conmutación de circuitos, 312-315
desconexión del circuito, 313
ejemplo, 314
encaminamiento, 380-382
encaminamiento alternativo, 381
establecimiento del circuito, 312-313

transferencia de datos, 313
redes de conmutación de paquetes:
control de congestión en, 418
encaminamiento en, 382-396
algoritmos de encaminamiento de primera generación, 392-393
algoritmos de encaminamiento de segunda generación, 393-394
algoritmos de encaminamiento de tercera generación, 394-396
características, 382-386
criterio de rendimiento, 383-384
ejemplos, 391-396
elementos de las técnicas de encaminamiento, 383
encaminamiento adaptable, 390-391
encaminamiento aleatorio, 389
encaminamiento estático, 386-387
estrategias de encaminamiento, 386-391
fuente de la información de red y tiempo de actualización, 385-386
instante de decisión, 384-385
inundación, 387-389
lugar de decisión, 384-385
redes de datos, congestión en, 407-443
redes públicas de telecomunicaciones, componentes de la arquitectura, 314
redes, y control de congestión, 419
redundancia de un código, 195
reflexión, 457
reflexión total interna, 107
refracción, 120-121
y transmisión en línea visual, 126
refugio de la retransmisión de celdas, 376
REJ dañado, 226-227
relación entre la energía de la señal por bit y la densidad de potencia del ruido, 86-87
relación señal-ruido (SNR), 85
relleno de bits, 231, 828
relleno de tráfico, 735
rendimiento, 162-163, 241-248
rendimiento de las microondas digitales, 112
repetición, 726
repetidor, 828
repetidores, 530-531
representante, 782-783
reserva, 496
respuesta de la red, 423
respuesta de usuario, 424
retardo de propagación, 828
retransmisión de celdas, 828
retransmisión de tramas, 16, 40, 341-345, 502, 828
arquitectura de protocolos, 342-343
plano de control, 342
plano de usuario, 343
fundamentos, 341-342
transferencia de datos de usuario, 343-345
retransmisión tras expiración del temporizador, 224
reutilización de frecuencias, 447-449
patrones, 448
revestimiento, 105
RF de banda estrecha con licencia, 567
RF de banda estrecha sin licencia, 567
RFC, 807-808
rotación circular, 495-496
RR dañado, 226
RSVP, *véase* protocolo de reserva de recursos (RSVP)
rendimiento de las microondas digitales, 112
ruido, 80-83, 828
diafonía, 82
ruido blanco, 828
ruido de intermodulación, 82, 828
ruido impulsivo, 82, 828
ruido térmico, 81

S

SA, *véase* asociaciones de seguridad (SA)
salto en frecuencia, 286
SAP de destino, cabecera de PDU de transporte, 27
SAP, *véase* punto de acceso al servicio (SAP)
SDH, *véase* jerarquía digital síncrona (SDH)
sectorización de celdas, 449-450
secuencia de comprobación de trama (FCS, *Frame Check Sequence*), 185, 233, 261, 828
secuenciación, 591
segmentación y reensamblado, interconexión de redes no orientada a conexión, 605-607
segmento TCP, 41
seguridad, 13
y selección del método de transmisión de datos, 77
seguridad de los computadores:
requisitos, 725
tecnología subyacente, 724-725
seguridad en red:
algoritmo de cifrado de clave pública RSA, 745-746
ataques activos, 726
ataques de denegación de servicio, 726
ataques pasivos, 725-726
autenticación de mensajes, 735-739
código, 736-737
función de dispersión de un solo sentido, 738-739
sin cifrar el mensaje, 736
usando cifrado simétrico, 736
capa de *sockets* segura (SSL, *Secure Sockets Layer*), 724, 749-754
arquitectura, 749-750
protocolo de alerta, 752

protocolo de cambio de especificación de cifrado, 751
protocolo de negociación bilateral, 752-754
capa de transporte segura (TLS, *Transport Layer Security*), 749
cifrado, 726-735
cifrado de clave pública, 742-744
cifrado simétrico, 727-728
estandar de cifrado avanzado (AES, *Advanced Encryption Standard*), 726
e integridad, 725
enmascaramiento, 726
firma digital, 744-745
funciones de dispersión seguras, 739-740
función de dispersión segura SHA-1, 739-740
requisitos, 739-740
IPSec, 754-759
ámbito, 755
aplicaciones, 754-755
asociaciones de seguridad (SA, *Security Associations*), 755-756
cabecera de autenticación, 756-758
encapsulado de la carga útil de seguridad, 758-759
modificación de los mensajes, 726
repetición, 726
requisitos relacionados, 725
y autenticación, 725
y confidencialidad, 725
y disponibilidad, 725
semántica, protocolo, 23
señal limitada en banda, 829
señal no periódica, 60
señal periódica, 60
señal portadora, 135
señales:
definición, 69
transmisión digital y analógica, 72-76
señales analógicas, 59, 72-76, 135, 829
ejemplos, 73-74
y datos, 75-76
señales de gestión de red, 321
señales digitales, 60, 72-76, 134-135
ejemplos, 73-74
y datos, 75-76
señalización, 829
definición, 69
señalización binaria explícita de congestión, 416
señalización de control, 319-329, 355-356
ATM:
canal de metaseñalización, 356
canal virtual de señalización usuario-red, 356
canal virtual de señalización usuario-usuario, 356
VCC semipermanente, 355
conmutación de circuitos, 319-329
funciones de señalización, 320-321
señalización por canal común, 322-326
ubicación de la señalización, 322
señalización por canal común, 322-326
definición, 323
desventajas, 325
modo asociado, 324
modo no asociado, 324
modos de operación, 324
principios, 323
señalización fuera de banda, 322
señalización intrabanda, 322
señalización intracanal, 322
sistema de señalización número 7, 326-329
elementos de una red de señalización, 327
estructuras de una red de señalización, 327-329
ubicación de la señalización, 322
señalización diferencial, 208
señalización digital:
ventajas, 72
señalización explícita de congestión, 415-416
categorías, 416
dirección, 416
señalización explícita de congestión basada en créditos, 416
señalización explícita de congestión basada en velocidad, 416
señalización explícita de congestión hacia adelante, 416
señalización explícita de congestión hacia atrás, 416
señalización fuera de banda, 322
señalización implícita de congestión, 415
señalización intrabanda, 322
señalización intracanal, 322
señalización polar, 136
señalización por canal común, 322-326, 829
definición, 323
desventajas, 325
modo asociado, 324
modo no asociado, 324
modos de funcionamiento, 324-325
principios, 323
señalización fuera de banda, 322-323
señalización intrabanda, 322-323
señalización intracanal, 322-323
señalización por canal común, modo asociado, 325
señalización unipolar, 136
servicio avanzado de telefonía móvil (AMPS, *Advanced Mobile Phone Service*), 460
servicio confirmado, 36
servicio de difusión pública (PBS, *Public Broadcasting Service*), 115
servicio de mejor esfuerzo, 367
servicio de red de entrega ordenada fiable, 681-690
servicio de red no fiable, 689-699

servicio de velocidad no especificada (UBR, *unspecified bit rate*), 350
servicio de velocidad variable en no tiempo real (nrt-VBR, *non real time Variable Bit Rate*), 350
servicio de velocidad variable en tiempo real (rt-VBR, *real time Variable Bit Rate*), 367
servicio no confirmado, 36
servicios ATM en no tiempo real, 366-368
  velocidad de tramas garantizada (GFR, *Guaranteed Frame Rate*), 367-368
  velocidad disponible (ABR, *Available bit Rate*), 367
  velocidad no especificada (UBR, *Unspecified Bit Rate*), 367
  velocidad variable en no tiempo real (nrt-VBR, *non real time Variable Bit Rate*), 366
servicios ATM en tiempo real, 365-366
  velocidad variable en tiempo real (rt-VBR, *real time Variable Bit Rate*), 366
    velocidad constante (CBR, *Constant Bit Rate*), 366
servicios diferenciados (DS, *Differentiated Services*), 665-674
  comportamiento salto a salto, 672-674
    PHB de reenvío asegurado, 673-674
    PHB de reenvío urgente, 672-673
  configuración, 670-672
  control de congestión, 669
  funcionamiento, 670-672
  mecanismos de acondicionamiento de tráfico, 671
    bloque de descarte de paquetes, 671
    clasificador, 671
    conformador, 671
    marcador, 671
    monitor, 671
  octeto, 668-670
  servicio de cola, 669
  servicios, 666-668
  terminología, 667
Shannon, Claude, 85
simulador de red *cnet*, 817-818
sincronización, 178
sincronización de trama, 216
sintaxis, protocolo, 23
sistema CRC-12, 189
sistema CRC-16, 189
sistema CRC-32, 189
sistema CRC-CCITT, 189
sistema de nombres de dominio (DNS, *Domain Name System*), 814
sistema de señalización número 7:
  elementos de la red de señalización, 327
    plano de control, 327
    plano de información, 327
    punto de señalización (SP, *Signaling Point*), 327
    punto de transferencia de señal (STP, *Signal Transfer Point*), 327
    y diseño de la red, 327
  estructuras de la red de señalización, 327-329
sistema de terminales de pequeña abertura (VSAT, *Very Small Aperture Terminal*), 115
sistema de transmisión, modelo de comunicaciones, 11
sistema final (ES, *End System*), 597
sistema intermedio (IS, *Intermediate System*), 597-598, 829
sistemas autónomos (AS, *Autonomous Systems*), 626-627, 629
sistemas con portadora analógica, 256-257
sistemas con portadora digital, 263-264
sistemas de telefonía celular analógica de primera generación:
  asignación de frecuencias, 460
  canales de control de AMPS, 461
  funcionamiento, 446
  módulo de asignación numérica (NAM, *Numeric Assignment Module*), 461
sistemas de telefonía celular analógicos de segunda generación, 461-470
  acceso múltiple por división de código (CDMA, *Code Division Multiple Access*), 462-463
  aspectos de diseño de CDMA móvil inalámbrico, 463-464
  comparación con sistemas de primera generación, 462
  enlace de ida en IS-95, 464-467
  enlace de retorno en IS-95, 467-470
sitio web de IPv6, 628
sitio web simple, 805,
sitio web sobre Ethernet de Charles Spurgeon, 540
SMTP, *véase* protocolo simple de transferencia de correo electrónico (SMTP)
SNMP, *véase* protocolo simple de gestión de red (SNMP)
Sociedad de Internet, 5
socket cliente, 814
socket servidor, 814
solicitud de equipos:
  cabecera de paquete, 43
  PDU de acceso a la red, 28
solicitud de repetición automática (ARQ, *Automatic Repeat Request*), 224-229, 829
  ARQ de parada y espera, 224-225
  ARQ de rechazo selectivo, 228-229
  ARQ vuelta atrás N, 226-228
sondeo y selección, 829
SONET (*Synchronous Optical Network*, red óptica síncrona), 19, 265
SONET/SDH, 265-267
  formatos de trama, 265-267
  jerarquía de señales, 265
SSL, *véase* capa de *sockets* segura (SSL)

subcapa de convergencia común (CPCS, *Common Part Convergence Sublayer*), 371
subcapa de segmentación y reensamblado (SAR, *Segmentation And Reasembly*), 370, 372
subportadora, 254
subredes, 42, 508, 597
subtipo *message*/*external-body* (mensaje/cuerpo-externo):
  MIME, 776
subtipo *message*/*partial* (mensaje/parcial):
  MIME, 775
subtipo *message*/*rfc*822 (mensaje/rfc822),
  MIME, 775
subtipo *multipart*/*alternative* (multiparte/alternativo), 775
subtipo *multipart*/*digest* (multiparte/resumen), 775
subtipo *multipart*/*mixed* (multiparte/mixto), 775
subtipo *multipart*/*parallel* (multiparte/paralelo), 775
suma de comprobación, 829
  cabecera TCP, 43
System Network Architecture (SNA), 29

T

tamaño de ráfaga contratado, 421
tamaño de ráfaga en exceso, 421
tasa de bits erróneos (BER, *Bit Error Rate*), 137, 138, 183, 829
tasa de error residual, 829
tasa de errores, 83, 829
tasa de información contratada (CIR, *Commited Information Rate*), 420-423
tasa del código, 195
TCP, 38, 41, 655, 656, 680, 699-707, 814
  control de congestión, 707-716
    gestión de ventana, 714-716
    gestión del temporizador de retransmisión, 707-714
  establecimiento de conexión, 703-704
  formato de cabecera, 699-703
  funcionamiento, 42-44
  gestión del temporizador de retransmisión:
    algoritmo de Karn, 713-714
    arranque lento, 714-715
    decaimiento exponencial de RTO, 713
    estimación de la variación del RTT, 709-713
    modificación dinámica del tamaño de ventana en caso de congestión, 715-716
    promediado simple, 708
    promedio exponencial, 708-709
  mecanismos, 703-704
  opciones de implementación de la política, 705-707
  parámetros de servicio, 702
  política de aceptación, 705-706
  política de confirmación, 706-707
  política de entrega, 705
  política de envío, 705
  política de retransmisión, 706
  primitivas de respuesta del servicio, 701
  primitivas de solicitud del servicio, 700
  segmento, 41-43
  servicios, 699
  terminación de conexión, 704
  transferencia de datos, 704
TCP orientado a conexión, 38
TCP/IP, 22, 29, 38, 40-45, 632
  aplicaciones, 44-45
  capa de acceso a la red, 40
  capa de aplicación, 41
  capa extremo a extremo (capa de transporte), 40-41
  capa física, 40
  capa Internet, 40
  capas, 40-41
  interfaces del protocolo, 45
  TCP y UDP, 41-42
    funcionamiento, 42-44
TD-CDMA, 471
TDM, *véase* multiplexación por división en el tiempo (TDM)
técnicas de aleatorización, 144-146
  bipolar con sustitución de 8 ceros (B8ZS, *Bipolar with 8-Zeros Sustitution*), 144-145
  bipolar de alta densidad de tres ceros (HDB3, *High Density Bipolar-3 zeros*), 145-146
técnicas de codificación de señales, 133-175
  datos analógicos, señales analógicas, 163-169
  datos analógicos, señales digitales, 157-163
  datos digitales, señales analógicas, 146-157
  datos digitales, señales digitales, 135-146
técnicas de comunicación de datos digitales, 177-213
  configuración de línea, 197-198
    topología, 197
    transmisión *full-duplex*, 197-198
    transmisión *half-duplex*, 197-198
  corrección de errores, 178, 191-197
    principios de los códigos de bloque, 193-197
  detección de errores, 178, 183-191
    comprobación de paridad, 184-185
    comprobación de redundancia cíclica (CRC, *Cyclic Redundancy Check*), 185-191
  errores, tipos de, 182-183
  interfaces, 198-209
    características de procedimiento, 199
    características eléctricas, 199
    características funcionales, 199
    características mecánicas, 199
    circuitos de intercambio, 199
    equipo terminación del circuito de datos (DCE, *data circuit-terminating equipment*), 199

equipo terminal de datos (DTE, *Data Terminal Equipment*), 199
interfaz física RDSI, 206-209
V.24/EIA-232-F, 200-206
interfaz, 178
sincronización, 178
transmisión asíncrona, 178, 179-181
transmisión síncrona, 178, 179, 181-182
técnicas de ecualización:
y distorsión de retardo, 80
tecnología de integración a muy gran escala (VLSI, *Very Large-Scale Integration*), 76
tecnología digital, y selección del método de transmisión de datos, 76
Telecomunicaciones Europeas Digitales sin Cable (DECT, *Digital European Cordless Telecommunications*), 472
telemática, 829
televisión por cable (CATV, *Community Antenna Televisión*), 104
telnet, 45, 632, 680, 814
temporización, 138
temporización, protocolo, 23
temporizador de retransmisión, 707-714
teorema de muestreo, 158
test de bucle local, 203
texto cifrado, 727, 744, 829
texto, datos digitales como, 71
texto nativo, 727, 743, 829
tiempo de vida de un datagrama, 605
tipo de audio, MIME, 776
tipo de carga útil (PT, *Payload Type*), 357
tipo de imagen, MIME, 776
tipo de mensaje:
MIME, 775-776
tipo *multipart* (multiparte), MIME, 773-775
tipo *text* (texto):
MIME, 773-775
tipo *video* (vídeo), MIME, 776
tolerancia a la variación del retardo de celda (CDVT, *Tolerance to CDV*), 435
tolerancia a ráfagas, 433
topología de la estructura, canal de fibra, 538
topología en anillo, 487-488
topología en árbol, 484-486
topología en estrella, 488
topología punto a punto, canal de fibra, 538
topologías, 829
canal de fibra, 537-539
LAN:
LAN en bus, 484
redes de área local (LAN, *Local Area Network*), 480
tráfico elástico, 655-656
tráfico inelástico, 656-657
requisitos, 656-657
tráfico internet, 654-657
trama, 181, 829
trama adecuada pero no elegible, 439
trama adecuada y elegible, 439
trama dañada, 226
trama de confirmación, 223
trama de datos, 222
trama de modo desconectado (DM, *Disconnected Mode*), 234
trama LAPB, 339
trama MAC, 491
control de acceso al medio en IEEE 802.3, 522-523
trama receptor preparado (RR, *Receiver Ready*), 236
tramas, 259
tramas de supervisión (tramas-S), 232
tramas informativas (tramas I), 232
tramas no numeradas (tramas-U), 234
transferencia de datos no orientada a conexión, 590, 829
transferencia de datos orientada a conexión, 829
transmisión analógica y digital, 76-78
datos, 69-72
señales, 72-76
transmisión analógica, 830
transmisión asíncrona, 178, 179-181, 830
transmisión balanceada, 208, 804
transmisión de celdas, 362-365
ATM:
capa física basada en celdas, 362-364
capa física basada en SDH, 364-365
capa física basada en celdas, 362-364
capa física basada en SDH, 364-365
transmisión de datos, 58,-93
capacidad del canal, 83-87
conceptos/terminología, 59-69
frecuencia, espectro y ancho de banda, 59-69
terminología de transmisión, 59
datos analógicos y digitales, 69-72
decibelios y potencia de la señal, 59
dificultades en la transmisión, 78-83
atenuación, 78-80
distorsión de retardo, 80
ruido, 80-83
medios, *véase* medios de transmisión
palabras clave, 136
señales analógicas y digitales, 72-76
terminología, 136
transmisión analógica y digital, 76-78
transmisión de datos analógicos mediante señales analógicas, 135, 157-163
índice de modulación, 164
modulación angular, 166-169
modulación en amplitud (AM), 163-166
transmisión de datos analógicos mediante señales digitales, 135, 157-163
modulación delta (DM), 160-163

modulación por impulsos de amplitud (PAM, *Pulse Amplitude Modulation*), 158-159
rendimiento, 162-163
transmisión de datos digitales mediante señales analógicas, 135, 146-157
modulación de amplitud en cuadratura, 156-157
modulación por desplazamiento de amplitud, 146-147
modulación por desplazamiento de fase, 149-153
modulación por desplazamiento de frecuencia, 147-149
rendimiento, 153-156
transmisión de datos digitales mediante señales digitales, 135-146
binaria multinivel, 140-141
definición, 135
esquemas bifase, 141-143
no retorno a cero (NRZ, *Non Return to Zero*), 139-140
señalización polar, 136
señalización unipolar, 136
técnicas de aleatorización, 144-146
velocidad de modulación, 136, 143-144
velocidad de transmisión, 136
transmisión, definición, 69 80
transmisión digital, 830
transmisión en línea visual, 122-126
absorción atmosférica, 124-125
multitrayectoria, 125-126
pérdidas en el espacio libre, 122-124
refracción, 126
transmisión en modo de corriente, 830
transmisión *full-duplex*, 59, 197-198, 830
transmisión *half-duplex*, 59, 197-198, 830
transmisión inalámbrica, 96
antenas, 110-117
infrarrojos, 117
medios, 59
microondas de satélite, 113-116
microondas terrestres, 112-113
radiodifusión, 116-117
transmisión no balanceada, 208, 830
transmisión simplex, 59, 830
transmisión síncrona, 178, 179, 181-182, 830
transmisiones de larga distancia mediante fibra óptica, 106
transmisor, modelo de comunicaciones, 11
transparencia de los datos, 231
transpondedores, 113
troncales de intercambio rurales, 106
troncales, red pública de telecomunicaciones, 314

U

UDP, 38, 41-42, 45, 680, 716-717
formato de cabecera, 716-717
funcionamiento, 42-44
no orientado a conexión, 38
UDP no orientado a conexión, 38
UMTS (*Universal Mobile Telecommunications System*, sistema universal de telecomunicaciones móviles), 471
unidad de datos del protocolo LLC, 491
unidad de datos del protocolo (PDU, *Protocol Data Unit*), 27, 30, 370, 491, 589-592, 830
unidifusión, 595, 664
e IPv6, 623-624
Unión Internacional de Telecomunicaciones, 3
uso de frecuencias prestadas, 449
usuario final, y control de congestión, 419
utilización de la capacidad, y selección del método de transmisión de datos, 77
utilización de un sistema de transmisión, 11

V

V.24/EIA-232-F, 200-206
circuitos de intercambio, 202
especificación de procedimiento, 204-205
especificación eléctrica, 200-201
especificación funcional, 201-204
especificación mecánica, 200
operación en modo de llamada, 206
variación del retardo de celda (CDV, *Cell Delay Variation*), 426-429, 433, 435
en la UNI, 428-429
VCC semipermanente, 355
vecinos internos, 651
velocidad constante (CBR, *Constant Bit Rate*), 350, 426, 432
velocidad de acceso, 420, 422
velocidad de celdas sostenible (SCR, *Sustainable Cll Rate*), 432
velocidad de modulación, 136, 143-144
velocidad de pico de celdas (PCR, *Peak Cell Rate*), 432
velocidad de tramas garantizada (GFR, *Guaranteed FrameRrate*), 367-368
velocidad de transmisión, 83
relación entre ancho de banda y, 66-69
velocidad de transmisión de una señal (velocidad de transmisión), 136
velocidad disponible (ABR, *Available Bit Rate*), 350, 367
velocidad no especificada (UBR, *Unspecified Bit Rate*), 367
velocidad primaria, 209
velocidad variable en no tiempo real (nrt-VBR, *non real time Variable Bit Rate*), 366
vendedores, 3
vídeo, 70

W

WAN, *véase* redes de área amplia (WAN)
W-CDMA, *véase* CDMA de banda ancha (W-CDMA)

X

X.25, 339-341
  circuito virtual, 340
  definición, 339
  nivel de enlace, 339
  nivel de paquete, 339
    funcionamiento, 341
  nivel físico, 339
  niveles, 339
    relación entre, 340
xDSL, 278-279
  alternativas, comparación, 279
  línea digital de abonado de alta velocidad (HDSL, *High Data Rate Digital Suscriber Line*), 278
  línea digital de abonado de muy alta velocidad (VDSL, *Very High Data Rate Digital Suscriber Line*), 279
  línea digital de abonado de una sola línea (SDSL, *Single Line Digital Suscriber Line*), 279

ACRÓNIMOS

Acrónimo	Término en inglés	Término en castellano
AAL	*ATM Adaptation Layer*	Capa de adaptación ATM
ADSL	*Asymmetric Digital Subscriber Line*	Línea de abonado digital asimétrica
AES	*Advanced Encryption Standard*	Estándar de cifrado avanzado
AM	*Amplitude Modulation*	Modulación en amplitud
AMI	*Alternate Mark Inversion*	Inversión de pulso alternada
ANS	*American National Standard*	Estándar nacional americano
ANSI	*American National Standard Institute*	Instituto de estandarización nacional americano
ARQ	*Automatic Repeat Request*	Solicitud de retransmisión automática
ASCII	*American Standard Code for Information Interchange*	Código estándar americano para el intercambio de información
ASK	*Amplitude-Shift Keying*	Modulación por desplazamiento de amplitud
ATM	*Asynchronous Transfer Mode*	Modo de transferencia asíncrono
BER	*Bit Error Rate*	Tasa de bits erróneos
B-ISDN	*Broadband ISDN*	RDSI de banda ancha
BGP	*Border Gateway Protocol*	Protocolo de pasarela fronteriza
BOC	*Bell Operating Company*	Compañía telefónica
CBR	*Constant Bit Rate*	Velocidad constante
CCITT	*International Consultative Committee on Telegraphy and Telephony*	Comité consultivo internacional telegráfico y telefónico
CIR	*Committed Information Rate*	Tasa información contratada
CMI	*Coded Mark Inversion*	Inversión de pulso codificada
CRC	*Cyclic Redundancy Check*	Comprobación de redundancia cíclica
CSMA/CD	*Carrier Sense Multiple Access with Collision Detection*	Acceso múltiple de portadora con detección de colisiones
DCE	*Data Circuit-Terminating Equipment*	Equipo terminación y del circuito de datos
DEA	*Data Encryption Algorithm*	Algoritmo de cifrado de datos
DES	*Data Encryption Standard*	Estándar de cifrado de datos
DS	*Differentiated Services*	Servicios diferenciados
DTE	*Data Terminal Equipment*	Equipo terminal de datos
FCC	*Federal Communications Commission*	Comisión federal de comunicaciones
FCS	*Frame Check Sequence*	Secuencia de comprobación de trama
FDM	*Frecuency-Division Multiplexing*	Multiplexación por división de frecuencia
FSK	*Frecuency-Shift Keying*	Modulación por desplazamiento de frecuencia
FTP	*File Transfer Protocol*	Protocolo de transferencia de archivos
FM	*Frecuency Modulation*	Modulación en frecuencia
GFR	*Guaranteed Frame Rate*	Velocidad de tramas garantizada
HDLC	*High-Level Data Link Control*	Control del enlace de datos de alto nivel
HTML	*HyperText Markup Language*	Lenguaje de marcas de hipertexto
HTTP	*HyperText Transfer Protocol*	Protocolo de transferencia de hipertexto
IAB	*Internet Architecture Board*	Junta de arquitectura de Internet
ICMP	*Internet Control Message Protocol*	Protocolo de mensajes de control de Internet
IDN	*Integrated Digital Network*	Red digital integrada
IEEE	*Institute of Electrical and Electronic Engineers*	Instituto de ingenieros eléctricos y electrónicos
IETF	*Internet Engineering Task Force*	Grupo de ingeniería de Internet
IGMP	*Internet Group Management Protocol*	Protocolo de gestión de grupos de Internet
IP	*Internet Protocol*	Protocolo Internet
IPng	*Internet Protocol—Next Generation*	Siguiente generación del protocolo Internet
IRA	*International Reference Alphabet*	Alfabeto de referencia internacional
ISA	*Integrated Services Architecture*	Arquitectura de servicios integrados
ISDN	*Integrated Services Digital Network*	Red digital de servicios integrados (RDSI)

Acrónimo	Término en inglés	Término en castellano
ISO	*International Organization for Standardization*	Organismo internacional de estandarización
ITU	*International Telecommunications Union*	Unión internacional de telecomunicaciones
ITU-T	*ITU Telecommunications Standardization Sector*	Grupo de estandarización de telecomunicaciones de la ITU
LAN	*Local Area Network*	Red de área local
LAPB	*Link Access Procedure—Balanced*	Procedimiento de acceso al enlace, balanceado
LAPD	*Link Access Procedure on the D Channel*	Procedimiento de acceso al enlace sobre el canal D
LAPF	*Link Access Procedure for Frame Mode Bearer Services*	Procedimiento de acceso al enlace para servicios en modo trama
LLC	*Logical Link Control*	Control del enlace lógico
MAC	*Medium Access Control*	Control de acceso al medio
MAN	*Metropolitan Area Network*	Red de área metropolitana
MIME	*Multi-Purpose Internet Mail Extension*	Extensiones multipropósito de correo electrónico
NRZI	*Non-Return to Zero, Inverted*	No retorno a cero, invertido
NRZL	*Non-Return to Zero, Level*	No retorno a nivel cero
NT	*Network Termination*	Terminador de red
OSI	*Open Systems Interconnection*	Interconexión de sistemas abiertos
OSPF	*Open Shortest Path First*	Primer camino más corto disponible
PBX	*Private Branch Exchange*	Centralita privada
PCM	*Pulse-Code Modulation*	Modulación por código de pulso
PDU	*Protocol Data Unit*	Unidad de datos de protocolo
PSK	*Phase-Shift Keying*	Modulación por desplazamiento de fase
PTT	*Postal, Telegrah and Telephone*	Correo, telégrafo y teléfono
PM	*Phase Modulation*	Modulación en fase
QAM	*Quadrature Amplitude Modulation*	AM en cuadratura
QoS	*Quality of Service*	Calidad de servicio
QPSK	*Quadrature PSK*	PSK en cuadratura
RBOC	*Regional Bell Operating Company*	Compañía telefónica regional
RF	*Radio Frecuency*	Radiofrecuencia
RSA	*Rivest, Shamir, Adleman Algorithm*	Algoritmo de Rivest, Shamir y Adleman
RSVP	*Resource ReSerVation Protocol*	Protocolo de reserva de recursos
SAP	*Service Access Point*	Punto de acceso al servicio
SDH	*Syncrhonous Digital Hierarchy*	Jerarquía digital síncrona
SDU	*Service Data Unit*	Unidad de datos del servicio
SMTP	*Simple Mail Transfer Protocol*	Protocolo simple de transferencia de correo
SNMP	*Simple Network Management Protocol*	Protocolo simple de gestión de red
SONET	*Syncrhonous Optical NETwork*	Red óptica síncrona
SS7	*Signaling System Number* 7	Sistema de señalización número 7
STP	*Shielded Twisted Pair*	Par trenzado apantallado
TCP	*Transmission Control Protocol*	Protocolo de control de transmisión
TDM	*Time-Division Multiplexing*	Multiplexación por división en el tiempo
TE	*Terminal Equipment*	Equipo terminal
UBR	*Unspecified Bit Rate*	Velocidad no especificada
UDP	*User Datagram Protocol*	Protocolo de datagrama de usuario
UNI	*User-Network Interface*	Interfaz usuario-red
UTP	*Unshielded Twister Pair*	Par trenzado no apantallado
VAN	*Value-Added Network*	Red de valor añadido
VBR	*Variable Bit Rate*	Velocidad variable
VCC	*Virtual Channel Connection*	Conexión de canal virtual
VPC	*Virtual Path Connection*	Conexión de camino virtual
WDM	*Wavelength Division Multiplexing*	Multiplexación por división de la longitud de onda
WWW	*World Wide Web*	Telaraña mundial

7ª Edición

Comunicaciones y Redes de Computadores

Stallings

Este *best-seller* internacional intenta proporcionar una visión unificada del amplio campo que comprenden las comunicaciones y redes de computardores.

El libro se ha organizado en las cinco partes siguientes:

Parte I. Visión general. Introducción
Parte II. Comunicaciones de datos
Parte III. Redes de área amplia
Parte IV. Redes de área local
Parte V. Arquitectura de comunicaciones y protocolos

Adicionalmente, el libro incluye un extenso glosario, una lista de los acrónimos más frecuentemente usados y una bibliografía. Cada capítulo incluye problemas y sugerencias de lecturas complementarias.

Los cambios más notables respecto a la anterior edidición son los siguientes:

- Comunicaciones inalámbricas y redes. El libro dedica ahora un capítulo a la tecnología de espectro, otro a las redes celulares inalámbricas y otro a las Lan inalámbricas.
- Ethernet Gigabit. La discusión sobre Ethernet Gigabit ha sido actualizada y se ha añadido una introducción a Ethernet a 10 Gbps.
- Servicios diferenciados.Esta edición prporciona un minucioso estudio de DS.
- Tasa de tramas garantizada. Desde la sexta edición se ha estandarizado un nuevo servicio ATM, denominado GFR, que ha sido específicamente diseñado para las subredes troncales IP. Esta edición proporciona una explicación de GFR y examina los mecanismos subyacentes en el servicio GFR.
- Conmutación de etiqueta multiprotocolo. MPLS ha emergido como una tecnología de gran importancia en Internet, siendo cubierta en esta edición.
- Detalles TCP/IP. Se ha añadido un nuevo capítulo básico sobre TCP e IP, reuniendo material iseminado en la sexta edición. Este material es vital para comprender la QoS y los aspectos de rendimiento de las redes basadas en IP.

Este libro va dirigido a una audiencia tanto académica como profesional. Para los profesionales interesados en este campo, el libro sirve como obra de referencia básica y es adecuado para autoestudio. Como libro de texto, puede usarse para un curso de uno o dos semestres.

LibroSite es una página web, en *castellano,* propia del libro que ofrece un respaldo académico exhaustivo, tanto para los docentes como para los alumnos. Los *profesores* pueden encontrar respuestas a los ejercicios, material adicional, sala de profesores, área de investigación, contribuciones, etc. Para los *estudiantes* existen ejercicios adicionales, enlaces a recursos de Internet sobre el tema, buscadores de trabajo, sala de estudio y mucho más.

www.librosite.net/stallings6

PEARSON Educación

www.pearsoneducacion.com

ISBN 978-84-205-4110-5